CISS 2008

Costas Array Generator Polynomials in Finite Fields

James K Beard

Life Senior Member, IEEE

jkbeard@ieee.org

http://jameskbeard.com

Overview

- Finite fields and Costas arrays
- Important properties of finite fields
- Costas arrays and the Difference Triangle
- Use of polynomials in finite fields to define a sequence of integers
  - When the sequence of integers is a permutation
  - When the sequence of integers is a Costas array
- New results
  - Definitions of spaces in *GF(q)* for Costas arrays
  - Progress in definition of Costas array space in *GF(q)*
- Other News
  - Costas array database extended to order 400
  - Progress report on search over order 27

Finite fields: Basis for Existing Costas array generators

- The Welch generator of singly-periodic Costas arrays
- The Lempel generator of symmetrical Costas arrays
- The Golomb generator of most other Costas arrays
- Golomb, Taylor, Rickard, Beard generalizations are based on these

Properties of Finite Fields

- Finite fields of order q, denoted by $GF(q)$
- Any implementation of $GF(q)$ is isometric to all other implementations
- $GF(q)$ exists only when $q=p^k$, p a prime, k>0
- Support commutative and associative addition, subtraction, multiplication, division
- In every $GF(q)$ there is a zero and a one
- Every element x has the property $x^q=x$
- 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
  - Each primitive element is of order $q-1$
  - Powers of each α_i cycle through all the nonzero elements
- Every element has the property $p \cdot x=0$

An Implementation of *GF(q)*

- Simplest example is integer arithmetic modulo a prime
- Vector extensions, $q=p^k$, $k>1$
  - We use polynomials of order $k-1$
  - Each polynomial coefficient is an integer modulo p
- Vector extension arithmetic is conventional polynomial arithmetic with additional operations
  - Result coefficients are taken modulo p
  - Polynomials that result from multiplication are taken modulo a *generating polynomial*
  - Division by x is multiplication by x^{q-2}
- The generating polynomial
  - Is monic and of order k
  - Is irreducible in *GF(q)*
  - Usually is selected so that x is a primitive element

Examples of Vector Extensions

- GF(27)
  - Generating polynomial x^3+2x+1
  - Twelve primitive elements, x, x^r, r does not contain factors of 26
- GF(64)
  - Generating polynomial x^6+x+1
  - Thirty-six primitive elements, x, x^r, r does not contain factors of 63
- Note that all elements in $GF(2^k)$ are their own negatives because $p \cdot x=0$

Polynomial Fit to a Sequence

- Polynomial is always of order *q-1* or less

$$\lambda_0 + \lambda_1 \cdot x + \lambda_2 \cdot x^2 + \ldots + \lambda_{N-1} \cdot x^{N-1} = \phi_x$$

- Express independent variable *x* and sum φ_x as powers p_j of a primitive element α

$$\sum_{i=0}^{N-1} \lambda_i \cdot \alpha^{i \cdot j} = \alpha^{p_j}, \quad j \in \{0 \ldots N-1\}$$

- Express this in vector-matrix notation

$$M \cdot \underline{l} = \underline{gp}$$

CISS 2008

The Vandermonde Matrix

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

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

The Order *q-1* Vandermonde Matrix

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

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

Values of |*M*| for q to 400

q-1	log(|M|)	Val(M)	q-1	log(|M|)	Val(M)	q-1	log(|M|)	Val(M)	q-1	log(|M|)	Val(M)
2	0	1	60	45	50	156	117	28	270	135	270
3	0	1*	63	0	1*	162	0	1	276	207	60
4	3	3	66	0	1	166	83	166	280	70	228
6	3	6	70	35	70	168	42		282	0	1
7	0	1*	72	18	27	172	129	93	288	72	
8	2		78	39	78	178	0	1	292	219	155
10	0	1	80	20		180	135	19	306	0	1
12	9	5	82	0	1	190	95	190	310	155	310
15	0	1*	88	22	34	192	48	112	312	78	25
16	4	13	96	24	22	196	147	14	316	237	114
18	0	1	100	75	91	198	99	198	330	0	1
22	11	22	102	51	102	210	0	1	336	84	148
24	6		106	0	1	222	111	222	342	171	
26	0	1*	108	81	76	226	0	1	346	0	1
28	21	17	112	28	98	228	171	107	348	261	136
30	15	30	120	30		232	58	144	352	88	311
31	0	1*	124	93		238	119	238	358	179	358
36	27	6	126	63	126	240	60	177	360	90	
40	10	32	127	0	1*	242	0	1*	366	183	366
42	0	1	130	0	1	250	0	1	372	279	269
46	23	46	136	34	100	255	0	1*	378	0	1
48	12		138	0	1	256	64	241	382	191	382
52	39	23	148	111	44	262	131	262	388	291	274
58	0	1	150	75	150	268	201	82	396	297	63

CISS 2008

Powers of *M* When |*M*|=1

$$M^2=(q-1)\cdot E=(p-1)\cdot E,\ M^4=(p-1)^2\cdot E^2=I$$

$$E=\begin{bmatrix}1&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\end{bmatrix},\ \text{interchanges rows or colums}$$

$$M^3=M^{-1}=(p-1)\cdot E\cdot M=(p-1)\cdot M\cdot E$$

Eigenvectors of *M*

$$M\cdot\left(I+M+M^{2}+M^{3}\right)=+\left(I+M+M^{2}+M^{3}\right),\ \lambda=+1$$

$$M\cdot\left(I-M+M^{2}-M^{3}\right)=-\left(I-M+M^{2}-M^{3}\right),\ \lambda=-1$$

$$M\cdot\left(I-j\cdot M-M^{2}+j\cdot M^{3}\right)=+j\cdot\left(I-j\cdot M-M^{2}+j\cdot M^{3}\right),\ \lambda=+j$$

$$M\cdot\left(I+j\cdot M-M^{2}-j\cdot M^{3}\right)=-j\cdot\left(I+j\cdot M-M^{2}-j\cdot M^{3}\right),\ \lambda=-j$$

The Lempel-Golomb Generators

- Form of the Lempel and Golomb generators

$$\alpha^{p_i} + \left(\alpha^k\right)^i = 1, \; 1 \le i \le q-2$$

- Lempel when *k=1*, Golomb when *k>1*
- Lempel Costas arrays are symmetrical

$$\lambda_i \begin{cases} = +1, & i = 0 \\ = -1, & i = k \\ = 0 \text{ otherwise} \end{cases}, \quad gp_i \begin{cases} = 0, & i = 0 \\ = p_{i-1}, & i > 0 \end{cases}$$

The Welch Generator

- Form of the Welch generator

$$\alpha^{i+r} = \left(p_i + 1\right) \cdot \alpha^0, \;\; 0 \le i \le q-1$$

- Produces Costas arrays of order *p-1*

$$\lambda_i \begin{cases} = +1, \;\; i = 1 \\ = 0 \text{ otherwise} \end{cases}, \;\; wp_i = \left(p_i + 1\right) \cdot \alpha^{-r}$$

- Offset *r* is arbitrary; these Costas arrays are singly periodic

CISS 2008

These Examples Raise Questions

- Classical generators produce trivially simple generator vectors
- The generalizations by Taylor, Rickard, and Beard are generalizations of these
- Is there a fundamental relationship that produces Costas arrays from simple generator vectors?
- What about non-generated Costas arrays?
- How do we find other generator vectors?

The Difference Triangle

- Description
  - Top row is column indices of a permutation
  - Successive rows are differences between indices in the top row
- This is our algebraic link between the Costas condition and Costas arrays
  - A base for backtrack programming searches
  - A way to check permutations for the Costas condition
- Pose the difference triangle in terms of generator polynomials

Definition: Difference Triangle

- Elements

$$d_{i,j} \begin{cases} = p_j, & i = 0 \\ = p_j - p_{j+i}, & i > 0 \end{cases}$$

- Example

Costas array:	2	4	0	3	1
Difference 1:	–2	4	–3	2	
Difference 2:	2	1	–1		
Difference 3:	–1	3			
Difference 4:	1				

The Value of the Difference Triangle

- Sequence is a permutation if
  - The elements of the first row are all between zero and *N-1*
  - None of the differences are zero
- Sequence is a Costas array if
  - There are no duplications in any difference row
  - Note that row *N-1* has only one element and thus is not relevant to the Costas condition

The Difference Triangle in *GF(q)*

- Pose each row of the generator equation

$$\text{Generator Equation:} \qquad M \cdot \underline{l} = \underline{gp}$$

$$\text{Row i:} \qquad \underline{rm}_i^T \cdot \underline{l} = gp_i = \alpha^{p_i}$$

- Each element p_i of the top row of the difference triangle is replaced by $\alpha^{(p_i)}$
- Difference rows become quotient rows
- Every element in the new difference triangle is α to the power of the corresponding element in the old difference triangle

CISS 2008

Elements of The Difference Triangle in *GF(q)*

- Equation for the elements

$$gd_{i,j}\begin{cases} = gp_j = \underline{rm}_j^T \cdot \underline{l} = \alpha^{p_j}, & i = 0 \\ = \dfrac{\underline{rm}_j^T \cdot \underline{l}}{\underline{rm}_{j+i}^T \cdot \underline{l}} = \alpha^{p_j - p_{j+i}} = \alpha^{d_{i,j}}, & 0 < i < N - j - 1 \end{cases}$$

- The number of difference elements is

$$\binom{N}{2} = \frac{N \cdot (N-1)}{2}$$

CISS 2008

Conditions for Permutation in *GF(q)*

- Top row may have no zeros
- None of the ratios in the difference rows may be the unity element

$$\frac{\underline{rm}_j^T \cdot \underline{l}}{\underline{rm}_{j+i}^T \cdot \underline{l}} \neq 1, \quad i > 0$$

- Preferred form for defining spaces

$$\left(\underline{rm}_j - \underline{rm}_{j+i}\right)^T \cdot \underline{l} \neq 0$$

CISS 2008

Costas Condition

- No duplications

$$\frac{\underline{rm}_j^T \cdot \underline{l}}{\underline{rm}_{j+i}^T \cdot \underline{l}} \neq \frac{\underline{rm}_{j+k}^T \cdot \underline{l}}{\underline{rm}_{j+i+k}^T \cdot \underline{l}}, \quad i,k > 0$$

- Clearing the denominators

$$\left(\underline{rm}_j^T \cdot \underline{l}\right) \cdot \left(\underline{rm}_{j+i+k}^T \cdot \underline{l}\right) \neq \left(\underline{rm}_{j+i}^T \cdot \underline{l}\right) \cdot \left(\underline{rm}_{j+k}^T \cdot \underline{l}\right)$$

- Preferred form for defining spaces

$$\underline{l}^T \cdot \left(\underline{rm}_j^T \cdot \underline{rm}_{j+i+k} - \underline{rm}_{j+i} \cdot \underline{rm}_{j+k}\right) \cdot \underline{l} \neq 0$$

Number of Row Differences

- Row *i* has *N-i* entries
- For *k* entries, there are $k \cdot (k-1)/2$ differences
- Thus row *i* has $(N-i) \cdot (N-i-1)/2$ differences
- Thus the number of differences is

$$N_{Costas} = \sum_{i=1}^{N-2} \frac{(N-i)\cdot(N-i-1)}{2} = \binom{N}{3}$$

An Issue with the Costas Condition

- The Condition is

$$\left(\underline{rm}_{j}^{T}\cdot\underline{l}\right)\cdot\left(\underline{rm}_{j+i+k}^{T}\cdot\underline{l}\right)-\left(\underline{rm}_{j+i}^{T}\cdot\underline{l}\right)\cdot\left(\underline{rm}_{j+k}^{T}\cdot\underline{l}\right)\neq 0$$

- Or

$$\alpha^{p_j}\cdot\alpha^{p_{j+i+k}}-\alpha^{p_{j+i}}\cdot\alpha^{p_{j+k}}=\alpha^{p_i+p_{j+k+i}}-\alpha^{p_{j+i}+p_{j+k}}\neq 0$$

- But exponentiation of any element is modulo *q-1* so that this condition cannot be met unless

$$p_j+p_{j+k+k}-p_{j+i}-p_{j+k}\neq 0 \bmod q-1$$

- Or

$$q\geq 2N-3$$

CISS 2008

What Do De Do About $N<q-2$?

- The classical generators
  - In the Lempel-Golomb generator, we set the extra element of *gp* to zero
  - There was no extra element in the Welch generator
- Our alternatives
  - Use a rank N submatrix of M and thus a shorter *l*
  - Set the extra elements of *gp* to zero
  - Define the remaining elements of *gp* to an arbitrary scheme such as an identity matrix

Identity Matrix for the Extra Elements

- Add an identity matrix of order *q*-*N*-2 as the lower right submatrix
- An additional constraint on $\underline{l}$ is

$$M_{N,q-2} \cdot \underline{l} = \underline{ls}_{N,q-2}$$

- Base vector $\underline{l}$ determining this submatrix is

$$\underline{l}_0 = M^{\#}_{N,q-2} \cdot \underline{ls}_{N,q-2}$$

$$M^{\#}_{N,q-2} = M^{T}_{N,q-2} \cdot \left[M_{N,q-2} \cdot M^{T}_{N,q-2} \right]^{-1}$$

Definition of the Matrix and Vector

$$
M_{N,q-2} = \begin{bmatrix} 1 & \alpha^{N} & \alpha^{2N} & \dots & \alpha^{(q-2)\cdot N} \\ 1 & \alpha^{N+1} & \alpha^{2\cdot(N+1)} & \dots & \alpha^{(q-2)\cdot(N+1)} \\ 1 & \alpha^{N+2} & \alpha^{3\cdot(N+2)} & \dots & \alpha^{(q-2)\cdot(N+2)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{q-2} & \alpha^{2\cdot(q-2)} & \dots & \alpha^{(q-2)\cdot(q-2)} \end{bmatrix}, \quad \underline{ls}_{N,q-2} = \begin{bmatrix} \alpha^{N} \\ \alpha^{N+1} \\ \alpha^{N+2} \\ \vdots \\ \alpha^{q-2} \end{bmatrix}
$$

Using the Conditions in *GF(q)*

- The permutation and Costas conditions
  - Constrain the space of $\underline{l}$
  - May be used as a basis to define a restricted space for $\underline{l}$
- This restricted space may be used to define a search of low complexity
- If the space can be shown to be null for a particular order, then this proves that there are no Costas arrays of that order

Condition on $\underline{l}$ When $N<q-1$

- Condition that $\underline{l}$ must satisfy is

$$M_{N,q-2} \cdot \left(\underline{l} - \underline{l}_0 \right) = \underline{0}$$

- Rank of this condition is q-N-1
- Call the vector space spanned by $M_{N,q-2}$ S_0
- The vector $\underline{l}$-$\underline{l}_0$ cannot be in S_0
- The vector $\underline{l}_0$ is zero if the extra elements of $\underline{l}$s are set to zero
- The issue goes away when a submatrix of M is used – extra elements of $\underline{l}$ are zero

Permutation Constraints in *GF(q)*

- The permutation condition is
  $$\left(\underline{rm}_j - \underline{rm}_{j+i}\right)^T \cdot \underline{l} \neq 0,\ \ i > 0$$
- The total constraint can be found by finding the intersection of each of these rank *N*-1 spaces
  - Call the rank 1 complement of each space: $SP_{j,i}$
  - Find the union *SPU* of these vector spaces
  - The vector $\underline{l}$ must be in the complement that space \SPU
- The space *SPU* can have a rank of up to *N*-1

CISS 2008

Costas Condition in *GF(q)*

- The Costas condition

$$\underline{l}^T \cdot \left(\underline{rm}_j^T \cdot \underline{rm}_{j+i+k} - \underline{rm}_{j+i} \cdot \underline{rm}_{j+k} \right) \cdot \underline{l} \neq 0, \;\; i,k > 0$$

- The vector $\underline{l}$ must be in the rank 2 space of each matrix in parenthesis
- The allowable space of $\underline{l}$ is the complement of the intersection of the complements all these rank 2 spaces
  - Complement the space of each constraint; call this rank *N*-2 space $SC_{j,l,k}$
  - Find the union of these rank 2 spaces; call this space *SCU*
  - The vector $\underline{l}$ must be in the complement of this space *\SCU*
- This space will have a rank of zero, one or two

Finding the Space of $\underline{l}$

- Find the complement of the allowed vector space of $\underline{l}$ as

$$SF = S_0 \bigcup SPU \bigcup SCU$$

- The vector space of $\underline{l}$ is the complement of this space

$$\underline{l} \in \backslash SF$$

- Definitions of the Spaces

$$S_0: \quad \underline{l} \notin M_{N,q-2} \cdot \left(\underline{l} - \underline{l}_o \right) \neq 0$$

$$SPU: \quad \underline{l} \notin \left(\underline{rm}_j - \underline{rm}_{j+i} \right)^T \cdot \underline{l} = 0,\ \ i > 0$$

$$SCU: \quad \underline{l} \notin \underline{l}^T \cdot \left(\underline{rm}_j \cdot \underline{rm}_{j+i+k} - \underline{rm}_{j+i} \cdot \underline{rm}_{j+k} \right) \cdot \underline{l} = 0,\ \ i,k > 0$$

Linear Algebra in *GF(q)*

- Method suggested by the definitions of the spaces
  - Construct unions by concatenating columns of vectors that span the null spaces of $\underline{l}$
  - Use Gram-Schmidt orthogonalization to find the rank
  - Use the orthogonal vectors to construct a matrix that spans the complement of the space
- The rank of the space of $\underline{l}$ will be zero, one or two
- If the rank is zero there are no Costas arrays of order N
- If the rank is one or two then any linear combination will generate Costas arrays

Self-Annihilating Vectors in *GF(q)*

- The dot product of a nonzero vector with itself may be zero
- Example

$$\underline{x}=\begin{bmatrix}\gamma^0\\ \gamma^1\\ \gamma^2\\ \vdots\\ \gamma^{q-1}\end{bmatrix},\ \left(\underline{x}^T\cdot\underline{x}\right)=\sum_{i=0}^{q-2}\gamma^{2i}\begin{cases}=\dfrac{1-\gamma^{2q-1}}{1-\gamma^2}, & \gamma^2\neq 1\\ =0, & \gamma^2=1\end{cases}$$

Dealing with Self-Annihilating Vectors

- They occur often in our work
  - All but two rows of *M* are self-annihilating
  - All <u>*gp*</u> corresponding to permutations are self-annihilating
- Orthogonalization won't work with self-annihilating vectors
  - Solution: Handle them in pairs
  - If two vectors aren't orthogonal, replace them in the matrix with their sum and difference
  - The new vectors won't be self-annihilating and will span the same space

Limitations of Linear Algebra

- Definition of the permutation condition space

$$\left(\underline{rm}_j - \underline{rm}_{j+i}\right)^T \cdot \underline{l} = 0,\ \ i > 0$$

- Definition of the Costas condition space

$$\underline{l}^T \cdot \left(\underline{rm}_j \cdot \underline{rm}_{j+i+k} - \underline{rm}_{j+i} \cdot \underline{rm}_{j+k}\right) \cdot \underline{l} = 0,\ \ i,k > 0$$

- The nature of these equations is Diophantine
  - The concept of magnitude isn't there in *GF(q)*
  - Only discrete values are allowed, ergo Diophantine equation concepts apply

Lessons Learned

- Note nature of constraints in terms of linear algebra principles
  - Permutation null space is rank 1, union over *j,i* is rank 1 to full rank; intuition tells us that it is low rank
  - Costas condition null space is rank 2, union over *j,i,k* is rank to to full rank; intuition tells us that it is high rank for larger *N*
- Tests in *GF(q)* contradict these interpretations
  - Posing the 56 Costas arrays of order 26 as <u>*gp*</u> in *GF(q)*, q=67, 71 and others and concatenating them as columns in order 26 matrices produces rank 25 or 26 matrices, not rank 0, 1 or 2 matrices
  - Q-R decomposition of Costas condition matrices in *GF(q)* produces vector spaces that do not conform to the original condition
- Odd observation: upper limit on *C(N)* of N^2 holds except for orders 5-23, holds exactly for order 256; this hints at a rank 2 generator!
- Conditions in *GF(q)* verified for known Costas arrays, but linear algebra derived results don't always check out the way they would in real or complex fields

Ongoing Work

- Find new ways to describe the spaces
  - Defined by the permutation condition
  - Defined by the Costas condition
  - Use wp_i instead of gp_i
- Find the union or intersection of the sets of the individual conditions
  - Linear algebra concepts led to focus on unions of sets
  - Diophantine concepts may lead to use of intersections of sets
- Examine the conditions as Diophantine equations

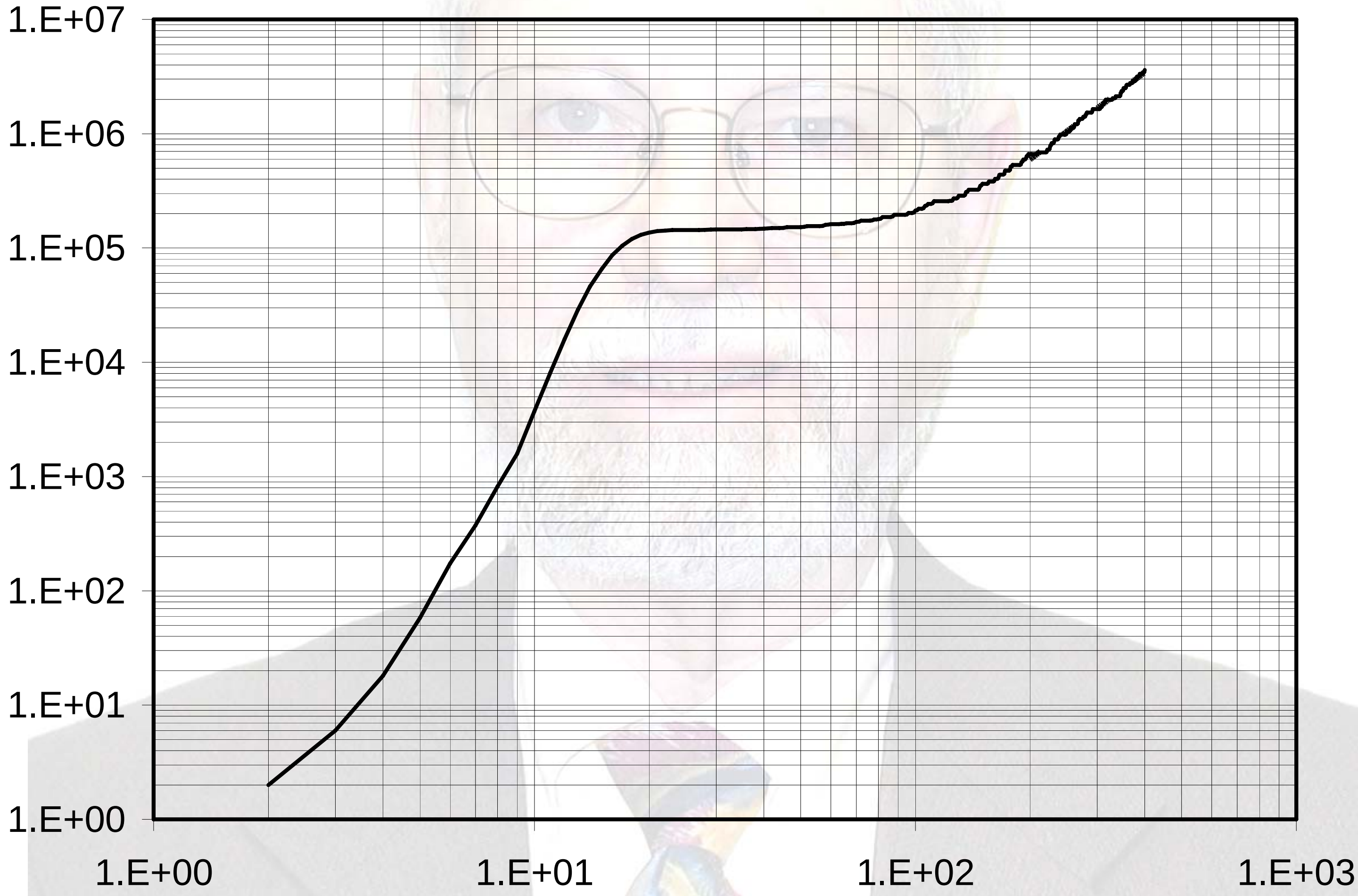
Summary

- We found simple linear algebraic equations in *GF(q)* for permutation and Costas conditions
  - Produced from difference triangle
  - Conditions found for validity, e.g. $q>2N-3$
  - Our equations are linear and quadratic
- Limitations on linear algebra concepts
  - Self-annihilating vectors common
  - Inverse and Q-R decomposition defined, SVD not defined
  - Some equations simply Diophantine in defining spaces

Other Related Work

- Database from CISS 2006 extended to order 400
  - Too large for single-sided data DVD: 6.9 GB
  - Available as 2.2 GB Zip archive on http://jameskbeard.com
  - Fit to cumulative curve, orders 200-400: $0.92143 \cdot (\text{Order})^{2.5253}$
- All-new interface
  - Designed to be run from HD for database on CD-ROM or HD (see below for screen shot)
  - Outputs CSV files for direct use by Matlab, Excel, C…
- Search over order 27
  - Not yet complete
  - We believe that the 196 Costas arrays of order 127 on the CISS 2006 database are all of them

Cumulative Distribution



Database Interface Screen Shot

```
Costas arrays from generators of order 2 to 400
Costas arrays of order  26, method: generated
*******************************************************************************
               Order          All    Essential   Symmetrical G-Symmetrical
                  22         2052          259             5           220
                  25           88           12             2             0
Current order:    26           56            8             2             0
                  27          196           28             7             0
                  28          712           89             0           336
*******************************************************************************
Current options:

No. Value, Description
1      F, T => all CAs to order 26; F => generated CAs to order 400
2     26, 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 C:\Data\IEEE\Papers\CISS2006\CDROM_Image\, Path for database top-level folder
9 Order_26, Pathname for output text

Enter option 1-9 to change, 10 for HELP, or 0 to proceed:
```

References

- Richard Bellman, *Introduction to Matrix Analysis*, Second Edition, SIAM Classics Series, ISBN 0-89871-399-4, p. 193 and 359-360.
- Solomon W. Golomb and Herbert Taylor, “Constructions and Properties of Costas Arrays,” *Proceedings of the IEEE* **72**, 9 (September 1984) 1143-2263.
- J. K. Beard, J. C. Russo, K. Erickson, M. Monteleone, and M. Wright, Costas Array Generation and Search Methodology, *IEEE Transactions on Aerospace and Electronic Systems*, **43**, 2 (April 2007), 522-538.
- J. K. Beard, Generating Costas Arrays to Order 200, *Conference on Information Sciences and Systems (CISS) 2006*, March 23, 2006, paper number 178, Princeton University.
- S. W. Golomb and G. Gong, The Status of Costas Arrays, *IEEE Trans. On Information Theory*, **53**, 11 (November 2007), 4260-4265.
- Jon Russo, Personal Communication.