A Probabilistic Approach on Estimating the Number of Modular Sonar Sequences

Ki-Hyeon Park and Hong-Yeop Song

{kh.park, hysong}@yonsei.ac.kr
Coding and Crypto Lab
Yonsei University, Seoul, KOREA

International Conference on Sequences and Their Applications (SETA) 2008,
University of Kentucky, Lexington
September 14-18, 2008

Call for Papers

2009 IEEE International Symposium on Information Theory (ISIT2009)

COEX, Seoul, Korea / June 28-July 3, 2009 / http://www.isit2009.info



The 2009 IEEE International Symposium on Information Theory will be held at COEX (Convention & Exhibition) in Seoul, Korea, from Sunday June 28 through Friday July 3, 2009. Seoul, the capital of Korea for more than 600 years, boasts its unique, dynamic mixture of tradition and modernity, offering a wide spectrum of activities for travelers.

Previously unpublished contributions across a broad range of topics in information theory are solicited, including (but not limited to) the following areas:

- Channel and source coding
- Coding theory and practice
- Communication theory and systems
- Cryptography and security
- Data compression
- Detection and estimation
- Emerging applications of information theory
- Information theory and statistics
- Network and multi-user information theory
- Pattern recognition and learning
- Quantum information theory
- Sequences and complexity
- Signal processing

Submitted papers should be of sufficient detail for review by experts in the field. In addition to submitting new results in areas that form the core of information theory, researchers in related fields and researchers working on novel applications of information theory are encouraged to submit contributions. Final papers will be five pages in length. The submission deadline is **January 7, 2009**. Detailed information on paper submission, technical program, tutorials, travel, social programs, and travel grants will be announced on the ISIT 2009 web site: **http://www.isit2009.info.**

General Co-chairs:

Jong-Seon No (Seoul National University, Korea) jsno@snu.ac.kr
H. Vincent Poor (Princeton University, USA) poor@princeton.edu

TPC Co-chairs:

Robert Calderbank (Princeton University, USA)
Habong Chung (Hongik University, Korea)
Alon Orlitsky (UCSD, USA)

For general inquiries, please contact the General Co-chairs.

TPC Members

J. Andrews
A. Asikhmin
R. Baraniuk
A. Barg
J. C. Belfiore
C. Berrou
E. Biglieri
N. Cai
C. Carlet
M. Chiang
S. Diggavi
A. El Gamal
H. El Gamal
E. Erkip
C. Fragouli
T. Fujiwara
M. Gastpar
V. Goyal
A. Grant
B. Hajek
B. Hassibi
T. Helleseth
T. Ho
T. Javidi
N. Jindal
I. Kontoyiannis
V. Kumar
J. N. Laneman
T. Linder
H. A. Loeliger
H. Lu
G. Lugosi
S. Meyn
O. Milenkovic
U. Mitra
R. Nowak
D. Palomar
M. Parker
B. Prabhakar
B. Preneel
K. Ramchandran
R. Roth
S. Savari
A. Scaglione
G. Seroussi
S. Shamai
D. J. Shin
A. Shokrollahi
P. Siegel
E. Soljanin
H. Y. Song
R. Srikant
W. Szpankowski
E. Telatar
L. Tong
D. Tse
E. Tuncel
D. Tuninetti
S. Ulukus
R. Urbanke
P. Viswanath
P. Vontobel
T. Weissman
F. Willems
R. Yeung

IEEE

In this talk

- A Brief Review about Sonar Sequences
- Initial Exhaustive Search
- Probabilistic Model
- Comparing Models with True Value
- Concluding Remarks

A Brief Review about Sonar Sequences

What is Sonar Sequence?

m=9										
8			•		•					
7	•									
6		•								
5				•			•			
4										
3								•	•	
2										
1										
0						•				
	1	2	3	4	5	6	7	8	9	n=9

- Can we select one dot for all columns to make no distinct two dots make same line segment?
- Upper picture is it-The integer sequence becomes: 7 6 8 5 8 0 5 3 3

A Brief Review about Sonar Sequences

Definition of Sonar Sequence and Modular Sonar Sequence

A function $f : A_n (\triangleq \{1, 2, ..., n\}) \rightarrow A_m$ has a distinct difference property (DDP) if for all integers h, i, and j, with $1 \leq h \leq n-1$ and $1 \leq i, j \leq n-h$,

$$f(i+h) - f(i) = f(j+h) - f(j) \quad \text{implies} \quad i = j. \tag{1}$$

And has a distinct modular difference property (DMDP) if

$$f(i+h) - f(i) = f(j+h) - f(j) \pmod{m} \quad \text{implies} \quad i = j. \tag{2}$$

Then a sequence with DDP is a Sonar Sequence, and it with DMDP is a Modular Sonar Sequence

A Brief Review about Sonar Sequences

Difference Triangle of Sonar Sequence

7		**6**		**8**		**5**		**8**		**0**		**5**		**3**		**3**
	-1		2		-3		3		-8		5		-2		0	
		1		-1		0		-5		-3		3		-2		
			-2		2		-8		0		-5		3			
				1		-6		-3		-2		-5				
					-7		-1		-5		-2					
						-2		-3		-5						
							-4		-3							
								-4								

- All row elements of each difference rows are distinct!

A Brief Review about Sonar Sequences

Difference Triangle of Modular Sonar Sequence

7		**6**		**8**		**5**		**8**		**0**		**5**		**3**		**3**
	8		2		6		3		1		5		7		0	
		1		8		0		4		6		3		7		
			7		2		1		0		4		3			
				1		3		6		7		4				
					2		8		4		7					
						7		6		4						
							5		6							
								5								

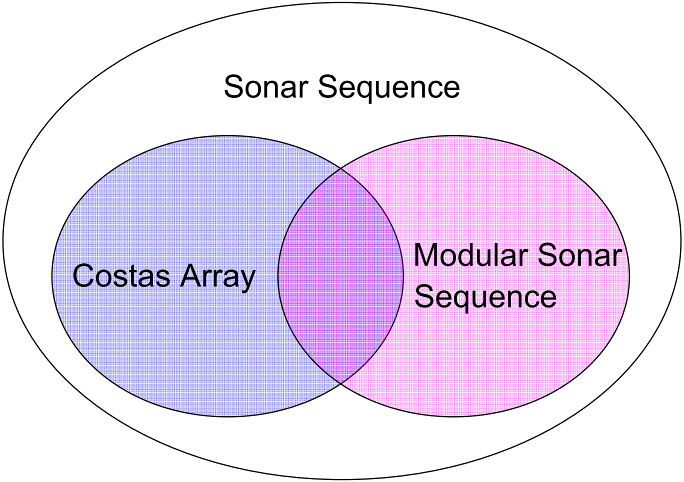
- All difference values are considered same when they are congruent by *mod* m at Modular Sonar Sequence. In this case, $m = 9$.

Why Modular Sonar Sequence?

- Usually, Sonar Sequences are for use in communication applications. Their optimum (maximum) length is $2m$, but it's hard to find good (long) sequences when m is large.
- Modular Sonar Sequences have some powerful construction methods that can reach their optimum length, $m+1$.
- They have some interesting and useful property, and are easy to analyze. Above all, they are easily converted and expanded to Sonar Sequences.

A Brief Review about Sonar Sequences

Relations between Sonar, Modular Sonar Sequences and Costas Arrays



A Brief Review about Sonar Sequences

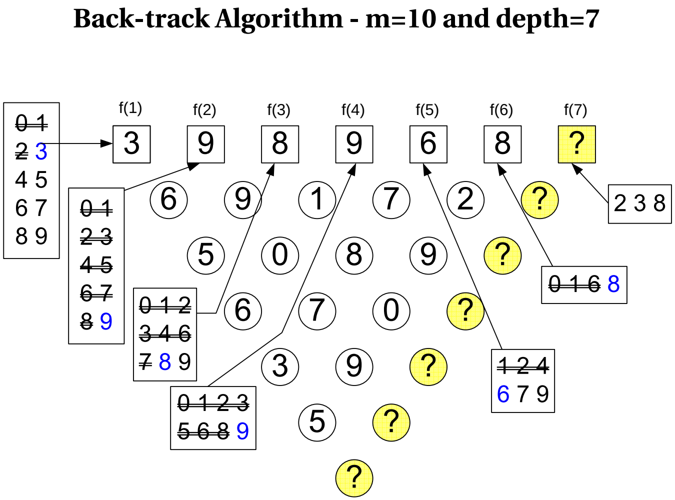
Some Properties and Algebraic Constructions of MSS

- Equivalant Sequences : If an f is a modular sonar sequence, the function g given by

$$g(i) = uf(i) + si + a, \quad i = 1, 2, \ldots, n \tag{3}$$

  is also a modular sonar sequence for all integer s and a, and for all integer u relatively prime to m.
- Reduction : Given an $m \times n$ (modular) sonar sequence, we can always have $m \times (n-1)$ (modular) sonar sequence by deleting the last term.
- Algebraic Constructions for $m \times (m+1)$ exist for $m = p$ and $m = p^k - 1$ for any prime p and a positive integer k.
  1. p : Quadratic Method, Extended Exponential Welch Method*
  2. $p^k - 1$: Shift Sequence Method

Initial Exhaustive Search



Initial Exhaustive Search

Object of Search

- The initial search was to answer the following two questions:

Q.1 Determine the maximum length n_{max} such that an $m \times n_{max}$ modular sonar array exists. What would be the maximum length n_e if we count only those that are NOT equivalent to any examples constructed by the three algebraic methods mentioned in the previous section and/or their reductions?

Q.2 Determine the number $I(m)$ of inequivalent sequences of length n_e for a given m, excluding those which are equivalent to the one given by the three algebraic constructions and/or their reductions.

Initial Exhaustive Search

Result of an Initial Search (part)

Description	m	n_{max}	n_e	$m-n_e$	$I(m)$
U	9	10	10	-1	3
SS	10	11			
Q,EEW	11	12	11	0	30
SS	12	13			
Q,EEW	13	14	13	0	17
U	14	14	14	0	2
SS	15	16	15	0	1
SS	16	17	16	0	1
Q,EEW	17	18	16	1	33
SS	18	19			
Q,EEW	19	20	17	2	321
U	20	18	18	2	136
U	21	19	19	2	17
SS	22	23			
Q,EEW	23	24			
SS	24	25			
U	25	22	22	3	4

SS:Shift Sequence **Q**:Quadratic **EEW**:Extended Exponential Welch **U**:Unidentified

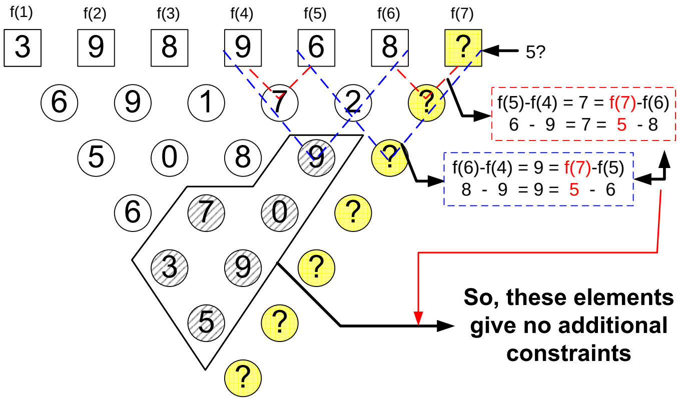
Initial Exhaustive Search

Two Observations of the Result

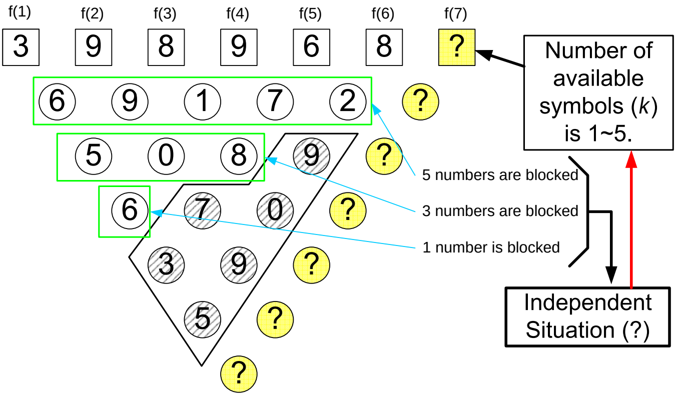
- $m - n_e$ is monotonically non-decreasing as m is increasing.
- $I(m)$ is decreasing as m is increasing for the range where the value $m - n_e$ remains the same.

Probabilistic Model

Back-track Algorithm - Remind



Probabilistic Model

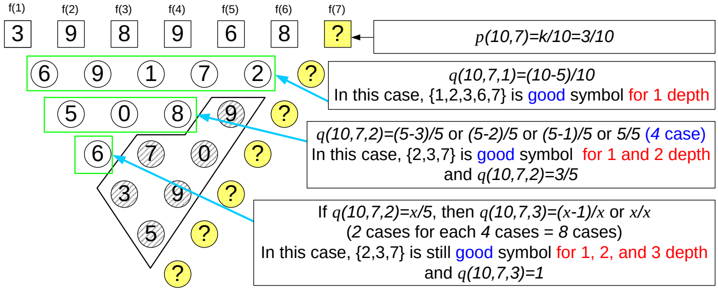


- We would like to estimate the number k even we do not know former terms.
- If the number of all 10×6 MSS is w, we could say the number of all 10×7 MSS is wk (?).

Probabilistic Model

Some Notations and Analysis

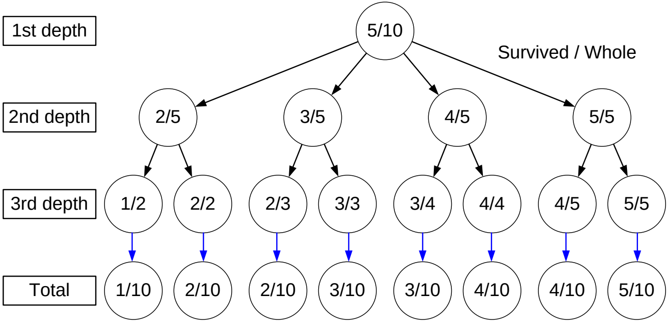
- $N(m,t)$ =The expected number of $m \times t$ Modular Sonar Sequences.
- $p(m,t)$ =The fraction of number of t-th symbol that give distinct value for whole difference rows.
- $q(m,t,h)$ =The fraction of number of t-th symbol that give distinct value for h-th difference row. m is modulo value for difference.



$p(10,7)=3/10=q(10,7,1)\times q(10,7,2)\times q(10,7,3)=5/10\times 3/5\times 1$

Probabilistic Model

General Case: m=10, t=7



- Total fraction is derived by the product of each fractions of depth on their path.
- Can we find one value for a row that can replace each cases with minimal error? In general m and t, can we find equation of m, t that estimates the true value well?

Probabilistic Model

Our Claim - Main Result

$$q(m,t,h) \approx 1 - \frac{m(t-2h)}{(m-h+1)^2}, \quad \text{for } 1 \le h \le \lfloor \tfrac{t}{2} \rfloor. \tag{4}$$

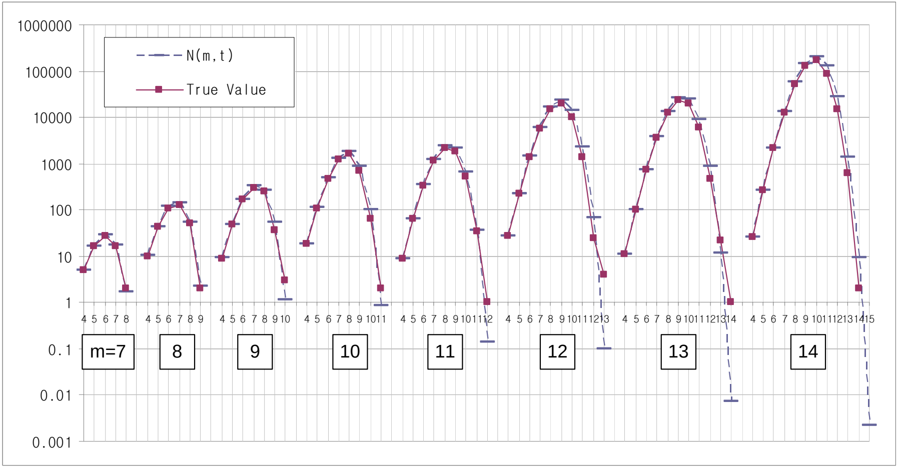
- And, since $p(m,t) \approx \prod_{h=1}^{\lfloor \frac{t}{2} \rfloor} q(m,t,h)$ and $N(m,n) \approx N(m,n-1)\,mp(m,n)$ by our assumptions,

$$\begin{aligned} N(m,1) &= m, \\ N(m,n) &\approx m^n \prod_{t=1}^{n} \prod_{h=1}^{\lfloor \frac{n}{2} \rfloor} \left(1 - \frac{m(t-2h)}{(m-h+1)^2}\right), \quad 2 \le n \le m+1. \end{aligned} \tag{5}$$

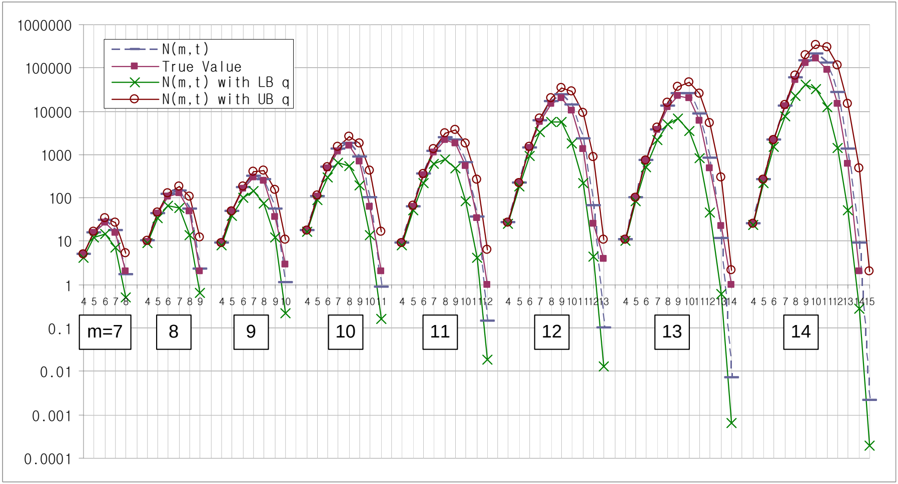
Comparing Models with True Value

m	n	TV	$N(m,n)$	m	n	TV	$N(m,n)$	m	n	TV	$N(m,n)$
7	4	5	5.00	10	9	707	895	13	5	100	100
	5	16	16.1		10	63	103		6	729	738
	6	27	29.5		11	2	0.857		7	3712	3842
	7	16	17.7	11	4	9	9.00		8	12433	13492
	8	2	1.73		5	64	64.1		9	22983	26184
8	4	10	10.5		6	343	350		10	20198	25321
	5	43	43.9		7	1152	1215		11	5922	8835
	6	108	118		8	2209	2479		12	481	852
	7	128	140		9	1857	2190		13	22	11.5
	8	50	54.3		10	533	670		14	1	0.0073
	9	2	2.26		11	35	37.1	14	4	26	26.0
9	4	9	9.33		12	1	0.142		5	262	262
	5	48	48.1	12	4	27	27.5		6	2160	2188
	6	167	173		5	222	223		7	12896	13362
	7	292	326		6	1399	1430		8	53373	57579
	8	249	271		7	5848	6187		9	130547	147892
	9	37	54.2		8	15324	17022		10	168576	209626
	10	3	1.12		9	20155	23392		11	87718	127056
10	4	18	18.0		10	10199	13865		12	14775	27624
	5	110	110		11	1351	2297		13	615	1362
	6	480	499		12	25	67.7		14	2	9.14
	7	1216	1325		13	4	0.0996		15	0	0.0022
	8	1619	1845	13	4	11	11.0				

Comparing Models with True Value

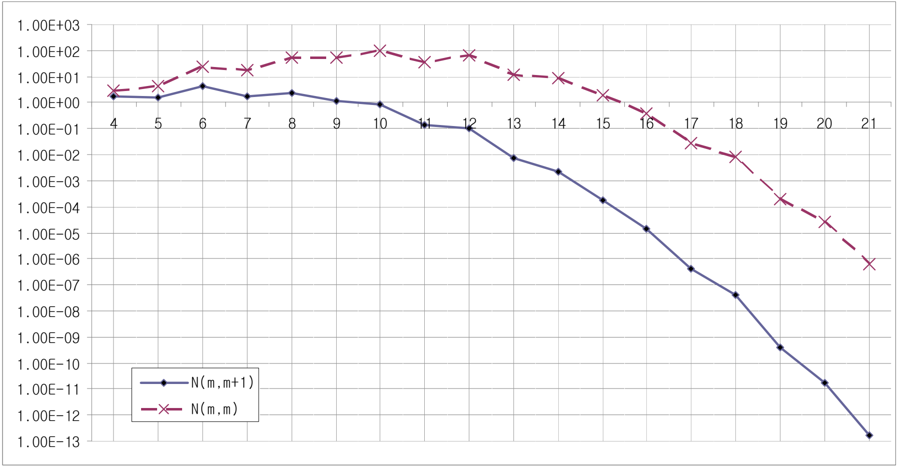


Comparing Models with True Value



Comparing Models with True Value

Why Decaying?



Concluding Remarks

- We have checked the existence of $m \times n$ modular sonar sequences by computer search for some small values of m
- We estimated the number of inequivalent examples for various values of m by probabilistic approach.
- From this estimate, we could have concluded that no full-size modular sonar sequence exists for m beyond a certain value. This is, however, not true.
- We could safely guess that any full-size example for large values of m must be either from an algebraic construction, or else the probability that it exists is extremely small.

Concluding Remarks

Some Unsolved Problems

1. Find an example of 35×35 modular sonar sequences (mod 35) or prove that none exists.
2. Generalize the above to the case of $m = p(p+2)$ being a product of twin primes.
3. Find infinitely many values of m for which an $m \times (m+1)$ modular sonar sequences do not exist.
4. Except for m being a prime or one less than a prime power, would the fact that the value in (5) is close to zero imply non-existence?
5. How accurate is the estimate in (5)?
6. Could a similar approach be used to estimate the number of Costas arrays?

Concluding Remarks

Thank You!

Any Questions?