

Finally, we do an exhaustive search to see if any 9-set can be extended to a code using the vertices in the corresponding list.

Example 4: The binary expressions of the numbers 4, 6, 9, 19, 26, 34, 53, 90, 93, 107, 108, 113, 118, 121 form a 2-identifying code \mathcal{C}_7 of length 7 and cardinality 14.

The binary expressions of the numbers 7, 9, 26, 36, 55, 63, 64, 85, 107, 114, 144, 163, 174, 185, 205, 211, 220, 222, 232, 244, 246 form a 2-identifying code \mathcal{C}_8 of length 8 and cardinality 21.

The binary expressions of the numbers in the next table form a 2-identifying code \mathcal{C}_9 of length 9 and cardinality 36.

8	9	22	49	60	76	91	98	116	133
152	166	171	189	195	204	222	232	253	270
272	291	301	327	375	377	383	406	411	416
450	466	469	486	493	506				

The binary expressions of the numbers in the next table form a 2-identifying code \mathcal{C}_{10} of length 10 and cardinality 63.

10	31	36	49	69	92	114	128	159	175
179	195	206	233	244	262	272	330	343	346
355	364	375	377	397	408	430	435	465	485
521	526	531	571	614	616	629	635	657	679
684	690	724	729	733	762	766	782	786	789
813	824	828	834	860	900	923	930	967	969
993	994	1021							

By adding to \mathcal{C}_{10} the binary expressions of the numbers 26, 62, 132, 205, 451, 467, 620, 624, 704, 718, 793, 1017 and removing 834 we get a 2-identifying code \mathcal{D}_{10} of cardinality 74. The code \mathcal{D}_{10} has the property that $\forall x \in F^{10} \exists c \in \mathcal{D}_{10} : d(x, c) = 2$. Theorem 4 shows that $\mathcal{D}_{10} \oplus F$ is 2-identifying of length 11 and cardinality 148.

By adding to \mathcal{C}_{10} the binary expressions of the numbers 132, 205, 451, 620, 624, 793, 1017 we get a 2-identifying code \mathcal{E}_{10} of cardinality 70. The code \mathcal{E}_{10} has the property that $\forall c \in \mathcal{E}_{10} : 1 \leq d(c, \mathcal{E}_{10} \setminus \{c\}) \leq 2$. Theorem 4 shows that $\mathcal{E}_{10} \oplus F^2$ is a 2-identifying code of length 12 and cardinality 280.

ACKNOWLEDGMENT

The authors wish to thank anonymous reviewers for careful reading and detailed comments which improved the quality of the paper.

REFERENCES

- [1] M. G. Karpovsky, K. Chakrabarty, and L. B. Levitin, "On a new class of codes for identifying vertices in graphs," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 599–611, 1998.
- [2] S. Ray, D. Starobinski, A. Trachtenberg, and R. Ungrangsi, "Robust location detection with sensor networks," *IEEE J. Sel. Areas Commun.*, vol. vi, 22, 2004, (Special Issue on Fundamental Performance Limits of Wireless Sensor Networks).
- [3] A. Lobstein, Identifying and Locating-Dominating Codes in Graphs, A Bibliography [Online]. Available: <http://perso.enst.fr/~lobstein/debut-BIBidetlocdom.pdf>
- [4] I. Honkala, M. G. Karpovsky, and L. B. Levitin, "On robust and dynamic identifying codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 599–611, 2006.
- [5] A. Frieze, R. Martin, J. Moncel, M. Ruszinkó, and C. Smyth, "Codes identifying sets of vertices in random networks," *Discr. Math.*, vol. 307, no. 9–10, pp. 1094–1107, 2007.
- [6] I. Charon, I. Honkala, O. Hudry, and A. Lobstein, "Structural properties of twin-free graphs," *Electron. J. Combin.*, vol. 14, no. 1, p. R16, 15, 2007.
- [7] J. Moncel, "Codes Identifiants Dans Les Graphes," Ph.D. dissertation, Université Joseph Fourier-Grenoble I, 2005.
- [8] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: Elsevier, 1997.

- [9] U. Blass, I. Honkala, and S. Litsyn, "Bounds on identifying codes," *Discr. Math.*, vol. 241, no. 1–3, pp. 119–128, 2001.
- [10] T. Laihonon, "Optimal codes for strong identification," *European J. Combin.*, vol. 23, no. 3, pp. 307–313, 2002.
- [11] M. Mollard, "Les Invariants du n -Cube," Thèse de 3ème Cycle, Université de Grenoble, Grenoble, France, 1981.
- [12] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 680–694, 1986.
- [13] S. M. Ranto, I. S. Honkala, and T. K. Laihonon, "Two families of optimal identifying codes in binary Hamming spaces," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1200–1203, 2002.
- [14] R. Struik, "Covering Codes," Ph.D. dissertation, Eindhoven University of Technology, Eindhoven, The Netherlands, 1994.
- [15] I. Honkala and A. Lobstein, "On identifying codes in binary Hamming spaces," *J. Combin. Theory Ser. A*, vol. 99, no. 2, pp. 232–243, 2002.
- [16] G. Exoo, "Computational results on identifying t -codes," Preprint.
- [17] M. G. Karpovsky, K. Chakrabarty, L. B. Levitin, and D. R. Avresky, "On the covering of vertices for fault diagnosis in hypercubes," *Inf. Process. Lett.*, vol. 69, no. 2, pp. 99–103, 1999.
- [18] G. Exoo, T. Laihonon, and S. Ranto, "New bounds on binary identifying codes," *Discr. Appl. Math.*, to be published.
- [19] U. Blass, I. Honkala, and S. Litsyn, "On binary codes for identification," *J. Combin. Des.*, vol. 8, no. 2, pp. 151–156, 2000.

The Status of Costas Arrays

Solomon W. Golomb, *Fellow, IEEE*, and Guang Gong, *Member, IEEE*

Abstract—The definition, the basic properties, and all the currently known systematic constructions for Costas arrays are presented, as well as a table of the number $C(n)$ of Costas arrays of order n , for $2 \leq n \leq 26$. It is proved that $\limsup_{n \rightarrow \infty} C(n) = \infty$, and the conjecture $\liminf_{n \rightarrow \infty} C(n) = 0$ is discussed. A Costas array of order n is known to be equivalent to a permutation of $\{1, 2, \dots, n\}$ for which the difference triangle contains no repeated elements in any row. A generalized Costas array of order $n = q - 1$ (or $n = q - 2$) is defined as a permutation of the nonzero elements (or also excluding 1) of the q -element field for which the difference triangle contains no repeated elements in any row. Two new constructions for these generalized Costas arrays are described and illustrated.

Index Terms—Costas array, difference triangle, generalized Costas array, permutation.

I. THE BASIC DEFINITIONS

A Costas array of order n , also called an $n \times n$ Costas array, is a subset C of size n of the n^2 lattice points (i, j) with $1 \leq i, j \leq n$, such that no two of the n lattice points in C are in the same row or column, and such that no two of the $\binom{n}{2}$ line segments between pairs of points in C agree in both magnitude and slope. Fig. 1 shows a Costas array of order 4.

The four points of the array are at $(1, 2)$, $(2, 1)$, $(3, 3)$, and $(4, 4)$. Among the six line segments connecting pairs of points, two have

Manuscript received April 26, 2007; revised July 30, 2007. The material in this correspondence was presented in part at the 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, March 2006.

S. W. Golomb is with the Department of Electrical Engineering—Systems, University of Southern California, Los Angeles, CA 90089-2565 USA (e-mail: sgolomb@usc.edu).

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@caliope.uwaterloo.ca).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2007.907524

4				•
3			•	
2	•			
1		•		
	1	2	3	4

Fig. 1. A Costas array of order 4.

TABLE I

THE NUMBER $C(n)$ OF COSTAS ARRAYS OF ORDER n

(Here $c(n)$ is the number of these inequivalent relative to the eight-element symmetric group of the square $n \times n$ array, and $s(n)$ is the number of symmetry Costas arrays of order n .)

n	$C(n)$	$c(n)$	$s(n)$
2	2	1	1
3	4	1	1
4	12	2	1
5	40	6	2
6	116	17	5
7	200	30	10
8	444	60	9
9	760	100	10
10	2160	277	14
11	4368	555	18
12	7852	990	17
13	12828	1616	25
14	17252	2168	23
15	19612	2467	31
16	21104	2648	20
17	18276	2294	19
18	15096	1892	10
19	10240	1283	6
20	6464	810	4
21	3536	446	8
22	2052	259	5
23	872	114	10
24	200	25	0
25	88	12	2
26	56	8	2

length $\sqrt{2}$, two have length $\sqrt{5}$, and two have length $\sqrt{13}$. However, whenever two line segments have the same length, their slopes are different. For example, the two segments of length $\sqrt{2}$, connecting $(1, 2)$ to $(2, 1)$ and $(3, 3)$ and $(4, 4)$, have respective slopes -1 and $+1$.

Costas arrays were introduced in [3] for applications to sonar and radar as frequency-hopping patterns. At each of n consecutive time intervals t_1, t_2, \dots, t_n , a different frequency is transmitted from a set of n adjacent frequencies f_1, f_2, \dots, f_n , in such a way that the ambiguity function (the two-dimensional autocorrelation function in both time and frequency), while having the value n at $(\Delta t, \Delta f) = (0, 0)$, has only the values 0 or 1 at any shift $(\Delta t, \Delta f) \neq (0, 0)$. This ideal (or thumb-tack) ambiguity function is best possible for determining the range (proportional to the time shift) and Doppler (the velocity to or from the observer, proportional to the frequency shift) of a target. This correspondence describe what is known, and not yet known, about constructions for Costas arrays, and a new generalization.

II. A SUMMARY OF APPROACHES

To date, two approaches have been followed to identify Costas arrays. One has been exhaustive search, by computer, to find all $n \times n$ Costas arrays, which has currently been completed for $n \leq 26$ [3], [13], [1], [2], [16] (also [17] for $n = 26$). (See Table I.) The other has been the discovery of specific constructions which provide examples of Costas arrays for many different values of n , [8]–[10]. All the specific construction methods which have been found are related to primitive roots in finite fields, or involve the opportunistic adjoining of an extra

“dot,” usually at a corner, to go from an example of size n to one of size $n + 1$.

For many years, $n = 32$ and $n = 33$ have been the smallest values for which no Costas arrays have been known [8]. The last publication that described new specific constructions appeared in 1992 [10]. If there are as yet undiscovered specific constructions, one possible way to identify them may be to look at examples found by exhaustive computer search that do not arise from any of the known constructions, and attempt to identify patterns in their formation. (Note. Interest in the research on Costas arrays has increased recently. There is a website [11] which provides a database for up-to-date publications or technical reports on Costas arrays, a survey article [5], and an invited talk on Costas arrays [7] given by the first author.)

III. KNOWN SYSTEMATIC CONSTRUCTIONS

A. The Welch Construction

For every prime $p > 2$, let g be any one of the $\phi(p - 1)$ primitive roots mod p , where ϕ is Euler’s ϕ -function. Then, the pairs (j, g^j) for $1 \leq j \leq p - 1$ are the coordinates of the points in an order $(p - 1)$ Costas array.

Since $(p - 1, g^{p-1}) = (p - 1, 1)$ is a “corner dot” of the foregoing Costas array, the row and column of this corner dot can be removed to obtain an order $(p - 2)$ Costas array.

Finally, if $g = 2$ is primitive mod p , which is believed (by Artin’s conjecture) to occur for a positive percentage of all prime numbers, $(1, 2)$ becomes a corner dot after the removal of the row and column of $(p - 1, 1)$, which may be removed (along with its row and column) to obtain an order $(p - 3)$ Costas array.

B. The Lempel Construction

For every finite field of $q > 2$ elements (where $q = p^k$, for all primes p and all positive integers k , such that $q > 2$), let α be any one of the $\phi(q - 1)$ primitive elements (i.e., generators of the multiplicative group) of $GF(q)$. Then the pairs (i, j) with $1 \leq i, j \leq q - 2$ such that $\alpha^i + \alpha^j = 1$ are the coordinates of the points in an order $(q - 2)$ Costas array. (Note that this Costas array is symmetric relative to the $i = j$ diagonal.)

When $q = p > 2$ is a prime, with the primitive root $\alpha = 2$, then $(i, j) = (q - 2, q - 2)$ is a corner dot which (together with its row and column) can be removed to give an order $(p - 3)$ Costas array, which is still symmetric relative to the $i = j$ diagonal. It is therefore distinct from the order $(p - 3)$ Costas array obtained from the Welch construction for the same prime p with primitive root 2. (Note that any Costas arrays obtained from the Welch construction are not symmetric relative to the $i = j$ diagonal. A detailed proof for this result can be found in [6], [4].)

C. The Golomb Construction

This is a generalization of the Lempel construction. Let α and β be any two primitive elements in the field $GF(q)$, and use the pairs (i, j) with $1 \leq i, j \leq q - 2$ as the coordinates of points in a Costas array whenever $\alpha^i + \beta^j = 1$. This gives an order $(q - 2)$ Costas array for all $q > 2$, which is the Lempel construction if and only if $\alpha = \beta$. (It is a rotation of the Lempel construction if $\alpha = \beta^{-1}$.) In general it is not symmetric.

By a theorem of Moreno *et al.* [12], proving a conjecture of Golomb [9], for every $q > 2$ it is possible to find primitive elements α and β in $GF(q)$ such that $\alpha + \beta = 1$. (Here α and β are not necessarily distinct.) In the Golomb construction, this yields an order $(q - 2)$ Costas array with $(1, 1)$ as a corner dot. Removing this corner dot, with its row and column, produces an order $(q - 3)$ Costas array for every $q > 2$ where $q = p^k$, p prime and $k \geq 1$.

In the special case $q = 2^k$, $k > 1$, from $\alpha + \beta = 1$ we also have $\alpha^2 + \beta^2 = 1$, so that $(2, 2)$ is also a point of the Costas array, which becomes a corner dot after $(1, 1)$, together with its row and column, is removed. When also $(2, 2)$, along with its row and column, is removed, a Costas array of order $(2^k - 4)$ results.

Proofs of the validity of the Welch, Lempel, and Golomb constructions are given in [8].

D. Taylor's T_4 Construction

If, in the field $\text{GF}(q)$, there is a primitive element α with $\alpha + \alpha^2 = 1$, then in the Lempel construction both $(1, 2)$ and $(2, 1)$ are points of the Costas array of order $q - 2$. Removing the two rows, and two columns, containing $(1, 2)$ and $(2, 1)$, an order $(q - 4)$ Costas array results.

In [10] it is shown that this situation arises for $q = 4, q = 5, q = 9$, and for those prime values of $q = p \equiv \pm 1 \pmod{10}$ where at least one of the roots of $x^2 + x - 1$ is a primitive root modulo p .

Note that $\alpha + \beta^2 = 1, \alpha^2 + \beta = 1$, with $\alpha \neq \beta$ leads to $\alpha - \beta = \alpha^2 - \beta^2, 1 = \alpha + \beta$, hence, $\alpha = \alpha^2$ and $\beta = \beta^2$, so α and β cannot be primitive modulo p for any prime p . (This rules out a possible generalization of the T_4 construction.)

E. The G_4 and G_5 Constructions

In the field $\text{GF}(q)$, if there are two primitive roots α and β with $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$, then also $\alpha^{-1} + \beta^2 = 1$, as shown in [10]. When this occurs, using the Golomb construction, since $\alpha^1 + \beta^1 = 1$, $(1, 1)$ is a corner dot which can be removed (together with its row and column), so that $(2, -1) = (2, q - 2)$ becomes a corner dot which can be similarly removed. Also, $(-1, 2) = (q - 2, 2)$ is now a corner dot, which can also be similarly removed. This process yields Costas arrays of successive orders $q - 2, q - 3, q - 4$, and $q - 5$. The values of q for which this construction occurs are $q = 4, q = 5, q = 9$, and those primes p for which the T_4 construction occurs which satisfy either $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$, as shown in [10].

F. A Construction of Very Limited Use

Another possible way to go from $n = q - 2$ successively to $n = q - 3$ and $n = q - 4$, for $n \times n$ Costas arrays, is to find two primitive roots α and β in $\text{GF}(q)$ where both $\alpha + \beta = 1$ and $\alpha^{-1} + \beta^{-1} = 1$, which would give dots at the diametrically opposite corners $(1, 1)$ and $(-1, -1) = (q - 2, q - 2)$. This actually occurs for $q = 7$, with $\alpha = 3$ and $\beta = 5$. (Here $\alpha^{-1} = 5$ and $\beta^{-1} = 3$, so that $\alpha + \beta \equiv \alpha^{-1} + \beta^{-1} \equiv 1 \pmod{7}$). However, this cannot work for any $q > 7$ for the following reason. From $\alpha + \beta = 1$ and $\alpha^{-1} + \beta^{-1} = 1$, we have $\beta = 1 - \alpha, \alpha^{-1} + (1 - \alpha)^{-1} = 1, \alpha^{-1}(1 - \alpha) + 1 = 1 - \alpha, \alpha^{-1} = 1 - \alpha$, and $\alpha^2 - \alpha + 1 = 0$. Thus, α is a root of $x^2 - x + 1$, which is a factor of $x^6 - 1$, so that $\alpha^6 = 1$. Given that α must be primitive, $q - 1 \leq 6$ and $q \leq 7$.

Essentially the same argument shows that if two primitive elements α and β in $\text{GF}(q)$ satisfy both $\alpha + \beta^{-1} = 1$ and $\alpha^{-1} + \beta = 1$ giving corner dots at $(1, q - 2)$ and $(q - 2, 1)$, then again $\alpha^2 - \alpha + 1 = 0, \alpha^6 = 1$, and α cannot be primitive for $q > 7$.

IV. ON THE ABUNDANCE OF COSTAS ARRAYS

A. Do Costas Arrays Become Extinct?

In [18], Silverman *et al.* presented a probabilistic argument to suggest that $C(n)$, the number of $n \times n$ Costas arrays, should go to 0 for large n . Indeed, as seen in Table I, the values of $C(n)$ for $2 \leq n \leq 26$, the value of $C(n)$ increases monotonically from $C(2) = 2$ to $C(16) = 21\,104$, beyond which it decreases monotonically down to $C(26) = 56$. The reduced number $c(n)$ of $n \times n$ Costas arrays when patterns which differ only by symmetries of the square are not

considered distinct, exhibits similar behavior, from $c(2) = 1$ up to $c(16) = 2648$ and then down to $c(26) = 8$. However, from Section III, we know that there are systematic constructions for $n \times n$ Costas arrays for arbitrarily large values of n , since the sequence of the prime numbers is infinite. The pessimistic assumption would be that for large n , only the examples obtained from these known constructions exist. By this reasoning, quite possibly $C(32) = C(33) = 0$.

B. $\limsup C(n) = \infty$ as $n \rightarrow \infty$

While it is possible, as just discussed, that $\liminf C(n) = 0$ as $n \rightarrow \infty$, it is provable that $\limsup C(n) = \infty$ as $n \rightarrow \infty$. Specifically, using only the Welch construction when $n = p - 1$, where p is prime, there are $\phi(p - 1)$ different primitive roots mod p , so that $C(p - 1) \geq \phi(p - 1)$ for every prime p . It is well known (see [15]) that $\phi(m) > m^{1-\epsilon}$ for all $m > m_0(\epsilon)$. Hence, the value of $C(n)$ becomes arbitrarily large as n takes the successive values $p_j - 1$, where p_j is the j th prime number.

C. Specific Large Values of $C(n)$

At $p = 65,537 = 2^{16} + 1$, the largest known Fermat prime, we have $p - 1 = 2^{16}$ and $\phi(p - 1) = 2^{15}$. Thus, from the Welch construction alone, $C(2^{16}) \geq 2^{15} = 32\,768$, an even larger number than $C(16) = 21\,104$. However, we can find a much bigger lower bound for $C(2^{16} - 1) = C(65,535)$. Specifically, there are still 2^{15} Costas arrays from the Welch construction at $p - 2$. In addition, from the Lempel and Golomb constructions, the number of ways to pick two primitive roots α and β , not necessarily distinct, from the set of 2^{15} such roots, is $\binom{2^{15}+1}{2} = 2^{14}(2^{15} + 1) = 536,887,296$, a lower bound for $C(65,535)$. As large as this number seems, it is microscopic in comparison with $65,535!$, the total number of permutation matrices of order $n = 65,535$.

D. General Large Values of $C(n)$

As already observed, since there are infinitely many primes, we can get $C(n) > x$ for any preassigned value of x by finding a prime p with $\phi(p - 1) > x$, and using the Welch construction for $n = p - 1$.

It is widely believed, though not yet proved, that there are infinitely many *twin primes*, integers p , and $r = p + 2$ that are both prime. Using the Golomb construction on the $\phi(r - 1)$ primitive roots modulo r to get order $r - 3 = p - 1$ Costas arrays, these will be distinct from the $\phi(p - 1)$ Welch constructions for order $p - 1$ Costas arrays. (The combined number depends on the number of pairs of primitive roots α and β , modulo r , with $\alpha + \beta = 1$.)

Generally, the largest contribution to $C(n)$ from systematic constructions occurs when $n = q - 2$ (where q is any power of any prime) using the Golomb construction with any two primitive roots α and β from the multiplicative group of $\text{GF}(q)$.

V. SEARCHING FOR OTHER SYSTEMATIC CONSTRUCTIONS

A. One Specific Possibility

The pairs (a, a^2) modulo p , for $1 \leq a \leq \frac{p-1}{2}$, for all primes $p > 2$, have the property that when plotted on a $\frac{p-1}{2} \times (p - 1)$ grid, all the vectors connecting pairs of these points are distinct. It is not clear whether these "semi-Costas arrays" can be extended to full Costas arrays, for some or all p , in any systematic way, or at all. Beside looking for pairs $(a, f(a))$ for $\frac{p-1}{2} \leq a \leq p - 1$ to complete the Costas array, the original $\frac{p-1}{2}$ points can be spaced twice as far apart, to provide either $(2a, a^2)$ or $(2a - 1, a^2)$, where the missing points to be provided for a full Costas array must be placed in the $\frac{p-1}{2}$ vacant columns. Even if this strategy can be made to work, the

resulting $n \times n$ Costas array has order $n = p - 1$, for which we already have the Welch construction.

B. Pattern Recognition

For values of n where all $n \times n$ Costas arrays have been found, it is possible to look at those which do not arise from any of the known systematic constructions, in order to see if any discernible pattern appears. The challenge here is to recognize a pattern even if there is one.

For example, in the Golomb construction with $\alpha^i + \beta^j = 1$, the plotted pairs have the form $(i, \log_\beta(1 - \alpha^i))$, where “ $\log_\beta(1 - \alpha^i)$ ” is an example of a *discrete logarithm*, to the base β , in the field of q elements. Since the “discrete logarithm problem” is known to be computationally hard, these pairs (i, j) would be very difficult to recognize as a pattern if one had not been told in advance. In fact, a reasonable cryptographic system could be based on encrypting numbers $i, 1 \leq i \leq q - 2$, by picking two primitive elements α and β from $\text{GF}(q)$, and setting $\pi(i) = \log_\beta(1 - \alpha^i)$, where π is a permutation on the set $\{1, 2, \dots, q - 2\}$.

Every $n \times n$ Costas array is a permutation on $\{1, 2, \dots, n\}$, but for large n very few permutations are Costas arrays. The Costas property can be verified by calculating the *difference triangle*, and checking that no row contains any repeated entry.

For example, $(i, 3^i)$ modulo 7 gives the permutation that maps $(1, 2, 3, 4, 5, 6)$ onto $(3, 2, 6, 4, 5, 1)$, and the difference triangle is

3,	2,	6,	4,	5,	1
-1,	4,	-2,	1,	-4	
	3,	2,	-1,	-3,	
	1,	3,	-5,		
		2,	-1,		
			-2		

with no repeated entry in any row.

On the other hand, the permutation $(2, 5, 4, 1, 3, 6)$ has the difference triangle

2,	5,	4,	1,	3,	6
3,	-1,	-3,	2,	3	
	2,	-4,	-1,	5,	
		-1,	-2,	2,	
			1,	1,	
				4	

Here we see a repeated “3” in the second row, and a repeated “1” in the fifth row. This corresponds to repeated vectors forming the sides of a parallelogram in the corresponding Costas-like array, violating the Costas property. This property of the difference triangle (no repeated entry in any row) is a necessary and sufficient condition for the permutation to be a Costas array. It may be helpful in recognizing new patterns which correspond to Costas arrays, and possibly in suggesting new patterns.

VI. OTHER INDEX SETS

The horizontal and vertical axes of a Costas array of order n are indexed with n consecutive integers, such as $1, 2, \dots, n$ or $0, 1, \dots, n - 1$. Designs analogous to Costas arrays can be described where the index sets on the two axes come from a different arithmetic system, e.g., from the additive group of the finite field $\text{GF}(p^k)$ with $k > 1$. For some parameter j , the index set is some $t(j)$, in $\text{GF}(p^k)$, and the pairs (x, y)

TABLE II
A PERMUTATION OF $\text{GF}(2^3)$

j	$x = (1+i)^j$	x^3	$(1+i)x^3$	$f(x) = x + (1+i)x^3$	s where $f(x) = (1+i)^s$
0	1	1	$1+i$	$-1+i$	7
1	$1+i$	$1-i$	-1	i	6
2	$-i$	i	$-1+i$	-1	4
3	$1-i$	$1+i$	$-i$	$1+i$	1
4	-1	1	$-1-i$	$1-i$	3
5	$-1-i$	$-1+i$	1	$-i$	2
6	i	$-i$	$1-i$	1	0
7	$-1+i$	$-1-i$	i	$-1-i$	5

TABLE III
THE DIFFERENCE TRIANGLE GIVEN BY $f(x)$

$-1+i$	i	-1	$1+i$	$1-i$	$-i$	1	$-1-i$
1,	$-1-i$	$-1+i$	i	-1	$1+i$	$1-i$	
$-i$	1	$-1-i$	$-1+i$	i	-1		
-1	$-1+i$	$1-i$	$-i$	1			
$-1+i$	i	-1	$1+i$				
$1+i$	$1-i$	$-i$					
$-1-i$	$-1+i$						
i							

of the *generalized Costas array* correspond to $\bar{x} = (x_j) = (t(j))$, and $\bar{y} = (y_j)$, which are some permutations of the elements (x_j) such that the difference triangle described in Section V-B has no repeated entries in any row. There may not actually be any mapping from the values of $t(j)$ onto the integers from 1 to n that will turn the generalized Costas array into an ordinary Costas array. In the following, we first describe this approach by an example. Then we will give two general constructions for generalized Costas arrays using linearized permutation polynomials.

Example 1: We consider a finite field $\text{GF}(3^2)$ which is defined by a primitive polynomial $h(x) = x^2 + x - 1$ over $\text{GF}(3)$. In the following, alternatively, we represent a primitive element $1 + i$ in $\text{GF}(3^2)$ analogous to the imaginary number i in the complex field (i.e., $i^2 = -1$). Let $f(x) = x + (1 + i)x^3$. Then $f(x)$ with $f(0) = 0$ is a permutation of $\text{GF}(3^2)$ as is shown in Table II.

We define an index set by $t(j) = (1 + i)^j$. Then the permutation $f(x), x = t(j), j = 0, 1, \dots, 7$ of $(t(j))$ has the difference triangle, as shown in Table III, with no repeated entry in any row. Thus, the pairs $(t(j), f(t(j))), j = 0, 1, \dots, 7$ form an order 8 generalized Costas array.

In the following, we set $q = p^k$ and let $\text{GF}(q)^*$ be the multiplicative group of $\text{GF}(q)$.

Construction A: Let α be a primitive element in $\text{GF}(q)$ where $k > 1$, and let an index set be $(t(j))$ where $t(j) = \alpha^j, j = 0, \dots, q - 2$. Let $f(x)$ be a linearized permutation polynomial of $\text{GF}(q)$, i.e., $f(x) = \sum_{j=0}^{k-1} c_j x^{p^j}$, where $c_j \in \text{GF}(q)$ is a permutation of $\text{GF}(q)$. Let $\text{gcd}(d, q - 1) = 1$, and $g(x) = f(x^d)$. Let the pairs $(x, g(x)), x = \alpha^j, j = 0, 1, \dots, q - 2$ be the coordinates of the points in the Cartesian plane $\text{GF}(q)^* \times \text{GF}(q)^*$.

Theorem 1: The above construction gives an order $(q - 1)$ generalized Costas array.

Proof: Since $\text{gcd}(d, q - 1) = 1$, then x^d is a permutation of $\text{GF}(q)$. Together with $f(x)$ being a permutation of $\text{GF}(q)$, it follows that $g(x) = f(x^d)$ is a permutation of $\text{GF}(q)$. Thus, we only need to show the difference triangle property. Let $a_j = f(\alpha^{dj}), 0 \leq j < q - 1$. Then we need to show that $T_s = \{a_{s+j} - a_j \mid j = 0, 1, \dots, (q-1) - s - 1\}$

has no repeated term for each s with $1 \leq s < q - 1$. Using the linearity of f , we have

$$\begin{aligned} a_{s+i} - a_i &= f(\alpha^{d(i+s)}) - f(\alpha^{di}) \\ &= f((\alpha^{d(i+s)} - \alpha^{di})) \\ &= f(\alpha^{di}(\alpha^{ds} - 1)). \end{aligned}$$

If there are two equal terms in T_s , say $a_{s+i} - a_i = a_{s+j} - a_j$ where $0 \leq i \neq j < q - 1 - s < q - 1$, applying the above identity and noting that $\gcd(d, q - 1) = 1$, we have

$$\begin{aligned} f(\alpha^{di}(\alpha^{ds} - 1)) &= f(\alpha^{dj}(\alpha^{ds} - 1)) \\ \implies \alpha^{di}(\alpha^{ds} - 1) &= \alpha^{dj}(\alpha^{ds} - 1) \\ \implies \alpha^{di} &= \alpha^{dj} \implies i = j \end{aligned}$$

which contradicts $i \neq j$. □

Remark: If $k = 1$, then $t(j)$ is an element in $\text{GF}(p)$, which can be regarded as a number in the range of $1, 2, \dots, p - 1$. Thus, the above construction for a generalized Costas array can be considered as a generalization of the Welch construction for $k > 1$.

From Construction A, the pairs $(\alpha^j, g(\alpha^j)), 0 \leq j < q$ can be described as the pairs $(\alpha^j, f(\beta^j)), 0 \leq j < q$ where both α and β are primitive elements in $\text{GF}(q)$. From this interpretation, we have the following construction which can be considered as a generalization of the Lempel and Golomb constructions indexed in $\text{GF}(q)^*$.

Construction B: Let both α and β be primitive elements in $\text{GF}(q)$, and $f(x)$ be a linearized permutation polynomial of $\text{GF}(q)$ with $f(1) = 1$. Let the pairs $(\alpha^j, \beta^{\tau(j)}), 1 \leq j < q - 1$ where $\alpha^j + f(\beta^{\tau(j)}) = 1$, be coordinates of the points in the Cartesian plane $E \times E$ where $E = \text{GF}(q) \setminus \{0, 1\}$.

Theorem 2: These coordinates form an order $(q - 2)$ generalized Costas array.

Proof: Note that $\beta^{\tau(j)}, 1 \leq j < q - 1$ is a permutation of E . We only need to show that $(\alpha^j, \beta^{\tau(j)}), 1 \leq j < q - 1$ satisfies the difference triangle property, i.e., a list of $\beta^{\tau(j+s)} - \beta^{\tau(j)}, 1 \leq j < q - 1 - s$ has no repeated elements for each $s, 1 \leq s < q - 1$. If there exist some $1 \leq i \neq j < q - 1 - s$ such that

$$\beta^{\tau(i+s)} - \beta^{\tau(i)} = \beta^{\tau(j+s)} - \beta^{\tau(j)},$$

applying f to both sides of the above identity and using the linearity of f , we have

$$f(\beta^{\tau(i+s)}) - f(\beta^{\tau(i)}) = f(\beta^{\tau(j+s)}) - f(\beta^{\tau(j)}).$$

By the definition, we have $f(\beta^{\tau(r)}) = 1 - \alpha^r$. Substituting this into the above identity, we have

$$\begin{aligned} 1 - \alpha^{i+s} - (1 - \alpha^i) &= 1 - \alpha^{j+s} - (1 - \alpha^j) \\ \implies \alpha^i(1 - \alpha^s) &= \alpha^j(1 - \alpha^s) \end{aligned}$$

which implies $i = j$, since $1 \leq s < q - 1$ and α is a primitive element in $\text{GF}(q)$. This contradicts $i \neq j$. □

We use an example to illustrate the result of Theorem 2.

Example 2: Let $\text{GF}(2^3)$ be defined by $x^3 + x + 1$, a primitive polynomial over $\text{GF}(2)$, and let α be a root of this polynomial in $\text{GF}(2^3)$. Let $f(x) = \alpha x + \alpha^2 x^2 + \alpha^5 x^4$. Then $f(x)$ is a linearized permutation polynomial of $\text{GF}(2^3)$ with $f(1) = 1$, which is as follows.

The pairs $(\alpha^i, \alpha^{\tau(i)}), i = 1, \dots, 6$ such that $\alpha^i + f(\alpha^{\tau(i)}) = 1$ where $\beta = \alpha$ are given by

i	$\alpha^i =$	$f(\alpha^i)$
	$c_0 + c_1\alpha + c_2\alpha^2$ (c_0, c_1, c_2)	
0	100	100
1	010	011
2	001	110
3	110	111
4	011	101
5	111	001
6	101	010

i	$\tau(i)$	$\alpha^{\tau(i)}$
1	2	001
2	4	011
3	6	101
4	3	110
5	1	010
6	5	111

001	011	101	110	010	111
010	110	011	100	101	
100	101	111	001		
111	001	010			
011	100				
110					

which has the following difference triangle: with no repeated entry in any row. Thus, these coordinates form an order 6 generalized Costas array.

REFERENCES

- [1] J. K. Beard, K. Erickson, and J. C. Russo, "Combinatoric collaboration on Costas arrays and radar applications," in *Proc. 2004 IEEE Radar Conf.*, Piscataway, NJ, 2004, pp. 260–265.
- [2] J. K. Beard, J. C. Russo, K. Erickson, M. Moneleone, and M. Wright, "Costas array generation and search methodology," *IEEE Trans. Aerosp. Electron. Eng.*, to be published.
- [3] J. P. Costas, "A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties," *Proc. IEEE*, vol. 72, no. 8, pp. 996–1009, Aug. 1984.
- [4] K. Drakakis, R. Gow, and L. O'Carroll, "On some properties of Costas arrays generated via finite fields," in *Proc. 40th Annu. Conf. Information Sciences and Systems (CISS 2006)*, Princeton, NJ, Mar. 2006, pp. 801–805.
- [5] K. Drakakis, "A review of Costas arrays," *J. Appl. Math.*, vol. 2006, pp. 1–32, 2006, Article ID 26385.
- [6] T. Etzion, "Combinatorial designs derived from Costas arrays," *Discr. Math.*, vol. 93, no. 23, pp. 143–154, Nov. 1991.
- [7] S. W. Golomb, "The status of Costas array constructions (invited talk)," in *Proc. 40th Annu. Conf. Information Sciences and Systems (CISS 2006)*, Princeton, NJ, Mar. 2006, pp. 822–824.
- [8] S. W. Golomb and H. Taylor, "Construction and properties of Costas arrays," *Proc. IEEE*, vol. 72, no. 9, pp. 1143–1163, Sep. 1984.
- [9] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combin. Theory (A)*, vol. 37, pp. 13–21, 1984.
- [10] S. W. Golomb, "The T_4 and G_4 constructions for Costas arrays," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1404–1406, Jul. 1992.
- [11] [Online]. Available: <http://www.costasarrays.org>
- [12] O. Moreno, "On primitive elements of trace equal to 1 in $\text{GF}(2^m)$," *Discr. Math.*, vol. 41, pp. 53–56, 1984.
- [13] O. Moreno *et al.*, "Survey of results on signal patterns for locating one or multiple targets," in *NATO Adv. Sci. Inst. Ser. C, Math. Phys. Sci.*, ser. Difference Sets, Sequences and their Correlation Properties, vol. 542 (1999), A. Pott, Ed. Bad Windsheim, Germany: NATO, 1998, p. 542.
- [14] S. W. Golomb and G. Gong, *Signal Design for Good Correlation*. New York: Cambridge Univ. Press, 2005.

- [15] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. New York: Oxford Univ. Press, 1980.
- [16] S. Rickard, "Searching for Costas arrays using periodicity properties," presented at the Conference on Mathematics in Signal Processing, Cirencester, U.K., Dec. 2004, unpublished.
- [17] S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade, "The enumeration of Costas arrays of size 26," in *Proc. 40th Annu. Conf. Information Sciences and Systems (CISS 2006)*, Princeton, NJ, Mar. 2006, pp. 815–817.
- [18] J. Silverman, V. E. Vickers, and J. M. Moody, "On the number of Costas arrays as a function of array size," *Proc. IEEE*, vol. 76, no. 7, pp. 851–853, Jul. 1988.

On the Error Exponents of ARQ Channels With Deadlines

Praveen Kumar Gopala, Young-Han Nam, and
Hesham El Gamal, *Senior Member, IEEE*

Abstract—In this correspondence, we consider communication over Automatic Repeat reQuest (ARQ) memoryless channels with deadlines. In particular, an upper bound L is imposed on the maximum number of ARQ transmission rounds. In this setup, it is shown that incremental redundancy ARQ outperforms Forney's memoryless decoding in terms of the achievable error exponents.

Index Terms—Erasure decoding, error exponents, incremental redundancy Automatic Repeat reQuest (ARQ), joint decoding.

I. INTRODUCTION

In [1], Burnashev characterized the maximum error exponent achievable over discrete memoryless channels (DMCs) in the presence of perfect output feedback. Interestingly, Forney has shown that even one-bit feedback increases the error exponent significantly [2]. More specifically, Forney proposed a memoryless decoding scheme, based on the erasure decoding principle, which achieves a significantly higher error exponent than that achievable through maximum likelihood (ML) decoding without feedback [3]. In Forney's scheme, the transmitter sends codewords of block length N . After receiving each block of N symbols, the receiver uses a reliability-based erasure decoder and feeds back one ACK/NACK bit indicating whether it has accepted/erased the received block, respectively. If the transmitter receives a NACK message, it then retransmits the same N -symbol codeword. After each transmission round, the receiver attempts to decode the message using **only** the latest N received symbols, and discards the symbols received previously. This process is repeated until the receiver decides to accept the latest received block and transmits an ACK message back to the transmitter.

It is intuitive to expect a better performance from schemes that do not allow for discarding the previous observations at the decoder, as compared with memoryless decoding. Our work here is concerned with one variant of such schemes, i.e., Incremental Redundancy Automatic Repeat reQuest (IR-ARQ) [4]. We further impose a deadline constraint in the form of an upper bound L on the maximum number of ARQ rounds.

Manuscript received August 8, 2006; revised April 10, 2007.

The authors are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: gopalap@ece.osu.edu; namy@ece.osu.edu; helgamal@ece.osu.edu).

Communicated by P. Viswanath, Associate Editor for Communications.

Color versions of Figures 1–3 in this correspondence are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TIT.2007.907431

In the asymptotic case $L \rightarrow \infty$, we argue that IR-ARQ achieves the same error exponent as memoryless decoding, denoted by $E_F(R)$. On the other hand, for finite values of L , it is shown that IR-ARQ generally outperforms memoryless decoding, in terms of the achievable error exponents (especially at high rates and/or small values of L). For example, we show that $L = 4$ is enough for IR-ARQ to achieve $E_F(R)$ for any binary symmetric channel (BSC), whereas the performance of memoryless decoding falls significantly short from this limit.

The rest of this correspondence is organized as follows. In Section II, we briefly review the memoryless decoding scheme without any delay constraints, and argue that allowing for memory in decoding does not improve the error exponent. The performance of the memoryless decoder and the incremental redundancy scheme, under the deadline constraint, is characterized in Section III. In Section IV, we consider specific channels (like the BSC, VNC and AWGN channels) and quantify the performance improvement achieved by incremental redundancy transmission. Finally, some concluding remarks are offered in Section V.

II. THE ARQ CHANNEL

We first give a brief overview of the memoryless decoding scheme proposed by Forney in [2]. The transmitter sends a codeword \mathbf{x}_m of length N , where $m \in \{1, \dots, M\}$. Here M represents the total number of messages at the transmitter, each of which is assumed to be equally likely. The transmitted codeword reaches the receiver after passing through a memoryless channel with transition probability $p(y|x)$. We denote the received sequence as \mathbf{y} . The receiver uses an erasure decoder which decides that the transmitted codeword was \mathbf{x}_m iff $\mathbf{y} \in \mathcal{R}_m$, where

$$\mathcal{R}_m = \left\{ \mathbf{y} : \frac{p(\mathbf{y}|\mathbf{x}_m)}{\sum_{k \neq m} p(\mathbf{y}|\mathbf{x}_k)} \geq e^{NT} \right\} \quad (1)$$

where $T \geq 0$ is a controllable threshold parameter. If (1) is not satisfied for any $m \in \{1, \dots, M\}$, then the receiver declares an erasure and sends a NACK bit back to the transmitter. On receiving a NACK bit, the transmitter repeats the codeword corresponding to the same information message. We call such a retransmission as an ARQ round. The decoder discards the earlier received sequence and uses only the latest received sequence of N symbols for decoding (memoryless decoding). It again applies the condition (1) on the newly received sequence and again asks for a retransmission in the case of an erasure. When the decoder does not declare an erasure, the receiver transmits an ACK bit back to the transmitter, and the transmitter starts sending the next message. It is evident that this scheme allows for an infinite number of ARQ rounds. This scheme can also be implemented using only one bit of feedback (per codeword) by asking the receiver to only send back ACK bits, and asking the transmitter to keep repeating continuously until it receives an ACK bit. Since the number of needed ARQ rounds for the transmission of a particular message is a random variable, we define the error exponent of this scheme as follows.

Definition 1: The error exponent $E(R)$ of a variable-length coding scheme is defined as

$$E(R) = \limsup_{N \rightarrow \infty} \frac{\log \Pr(E)}{\bar{\tau}} \quad (2)$$

where $\Pr(E)$ denotes the average probability of error, R denotes the average transmission rate, and $\bar{\tau} = (\ln M/R)$ is the average decoding delay of the scheme, when codewords of block length N are used in each ARQ transmission round.