Cyclic Code Weight Enumeration in the Transform Domain

Jean Conan and Francis Langlois

Département de génie électrique, Ecole Polytechnique de Montréal
C.P. 6079 - Succ. "A", Montréal, P.Q., Canada, H3C 3A7

RÉSUMÉ

Lorsque n et q sont relativement premiers entre eux et m représente l'ordre multiplicatif de q modulo n, les mots d'un code cyclique sur GF(q) de longueur n peuvent etre associés à des n-uples sur GF(q^m) par une transformation de Galois-Fourier basée sur une racine primitive $n^{ième}$ de l'unité sur GF(q^m). On demontre que la cyclicité du code se traduit par l'annulation d'un certain nombre de composantes spectrales dont les indices de position appartiennent à une réunion de q-orbites de Z_n. Dans le cas des codes minimaux, une seule orbite entre en jeu à partir de laquelle il devient aisé d'identifier des représentants, dans le domaine spectral, des cycles élémentaires. Le poids de Hamming des mots de code correspondants est alors aisément calculable, sans inversion de Fourier, par utilisation soit de l'algorithme d'Euclide soit d'une procédure d'approximation rationnelle minimale d'une séquence scalaire (p.e. la procédure de Wilkinson-Morf-Kailath). Les résultats sont d'ailleurs extensibles au cas général par adaptation au cas spectral d'un ,résultat du à Van Lint. Du fait de l'efficacité des procédures de calcul des transformées de Galois-Fourier, l'approche devrait s'avérer capable de décomposer des codes de dimensions beaucoup plus importantes que les valeurs atteintes par les méthodes classiques.

SUMMARY

Given (n,q) = 1 and m the multiplicative order of q modulo n, cyclic codes over GF(q) with length n can be mapped into n-tuples over GF(q^m) through a Galois-Fourier transformation making use of a primitive nth root of unity of GF(q^m). It is shown that the cyclic property of the codes is reflected by the cancellation of specific spectral components corresponding to indices which belong to a union of q-chains of Z_n. For minimal cyclic codes only one q-chain is present from which it becomes easy to identify cycle representatives in the spectral domain. The Hamming weight of these specific codewords can be easily computed without Fourier inversion through the use of either Euclid's algorithm or any minimal partial realization procedure for rational sequences such as the Wilkinson-Morf-Kailath algorithm. The results are furthermore applicable to non minimal codes by using a spectral version of an extension of a result due to Van Lint and which is easily implementable on a computer. Taking into account the efficiency of computer based Fourier transformers, it is believed that this approach should be able to deal with larger codes than previously possible with the more classical direct methods.

I. Introduction

The search of the weight enumeration of a code generally requires an amount of computations growing exponentially with the dimension of the code. Cyclic codes, however, present a rich mathematical structure that may be exploited to reduce the amount of computations during the search and to allow the study of bigger codes. The methods which are known (Goethals [1]; Willett [2]; Tavares, Allard and Shiva [3]; and Cohen, Godlewski and Perrine [4]) are based on a partition of the set of codewords in elementary cycles, and the calculation of a unique representative codeword for each cycle, thus avoiding the systematic generation of all the codewords. We expose here a similar method which is based on the properties of the cyclic codes in the transform domain.

II Galois-Fourier transforms of codewords

Given n and q relatively primes and m the multiplicative order of q modulo n (i.e., the smallest integer m such that $q^m = 1 \bmod n$), we define the Galois-Fourier transform of the vector $\underline{c} = (c_0,c_1,\ldots,c_{n-1}) \in GF(q)^n$ as the vector $\underline{C} = (C_0,C_1,\ldots,C_{n-1}) \in GF(q^m)^n$ such that

$$C_k = \sum_{i=0}^{n-1} c_i \varsigma^{ik} \qquad k=0,1,\ldots,n-1$$

where ς is a primitive n^{th} root of unity in the extension field GF(q^m) and m is the multiplicative order of q modulo n. By analogy with real signal analysis, the vector spaces $GF(q)^n$ and $GF(q^m)^n$ are called, respectively, the time and the frequency domains while $\underline{C}$ is called the spectrum vector of $\underline{c}$.

The Mattson-Solomon polynomial associated with $\underline{c}$ will be defined as

$$C_{MS}(x) = \sum_{j=0}^{n-1} C_j x^{n-j} \bmod(x^n-1).$$

The necessary and sufficient conditions for a linear subset $GF(q^m)^n$ to be the spectrum vectors of a cyclic code over GF(q) can be expressed as follows:

(1) Conjugacy constraints: in order for a vector in $GF(q^m)^n$ to have its inverse Galois-Fourier Transform in $GF(q)^n$, its components must satisfy:

$$C_k^q = C_{((qk))}$$

where ((qk)) means that qk must be reduced modulo n.

(2) For a given code, specific spectral components are always zero.

A set of spectral components which are related to one another by conjugacy constraints is called an orbit. Components that share the same orbit have subscripts which belong to the same cyclotomic set of Z_n. Thus, we can say that a cyclic code is a code that has nul orbits, and at least one non-zero orbit.

III Weight enumeration of minimal codes

Minimal cyclic codes are characterized by parity check polynomials which are irreducible over GF(q) and whose roots over GF(q^m) are the successive powers of some primitive element in GF(q^m). Hence the associated set of power values form a cyclotomic subset of Z_n which is precisely the set of indices where the Galois-Fourier components are non zero. Hence the spectrum vectors of minimal codes have only one non-zero orbit. Thus, knowing only one non-zero component, we can use the condition (1) to find all the elements of $GF(q^m)$ that are "allowed" to be in the spectrum vector. The cycle representatives are then, among the allowed elements, the ones that may not belong to the same cycle, that is, elements such that the differences of their logarithms are not multiples (modulo n) of their subscript.· This last property comes from the fact that a time-domain cyclic shift corresponds to a frequency-domain modulation (i.e., $C_j \rightarrow \varsigma^j C_j$).

Example:

Take the minimal code M(15,4), with generator polynomial corresponding to the codeword $\underline{c}$ = (110001100011000). We find:

$$\underline{C} = (0,0,0,\alpha^{14},0,0,\alpha^{13},0,0,\alpha^{7},0,0,\alpha^{11},0,0),$$

where α is a primitive element of $GF(2^4)$. The cyclotomic set containing the subscripts of the non-zero orbit of the code is {3,6,9,12}. By condition (1), we must have:

$$C_3^2 = C_6,\ C_6^2 = C_{12},\ C_{12}^2 = C_9,\ \text{and } C_9^2 = C_3,$$

that is:

$$C_3^{16} = C_3,\ \text{or } C_3^{16} - C_3 = 0$$

Thus, each element of $GF(2^4)$ is "allowed" to be in the spectrum vectors. Cycle representatives may now be found as follows. The multiples of 3, modulo 15, are { 0,3,6,9,12,15 }. One can then easily check that { $\alpha^0,\alpha^1,\alpha^2$ } have logarithms whose differences are not multiples of 3. We then choose, as cycle representatives:

$$\underline{R}_0 = (0,0,0,\alpha^0,0,0,\alpha^0,0,0,\alpha^0,0,0,\alpha^0,0,0)$$

$$\underline{R}_1 = (0,0,0,\alpha^1,0,0,\alpha^2,0,0,\alpha^8,0,0,\alpha^4,0,0)$$

$$\underline{R}_2 = (0,0,0,\alpha^2,0,0,\alpha^4,0,0,\alpha^1,0,0,\alpha^8,0,0)$$

Since the weight of a codeword is the number of n^{th} root of unity that are not zeros of the Mattson-Solomon polynomial so that $w(\underline{c})$ = n-g.c.d. $(C(2),Z^n-1)$, the weight of a frequency-domain cycle representative can be obtained either by Euclid's algorithm or by minimal partial realization of sequences. This reduces substantially the amount of computation that would be needed by the use of the inverse Galois-Fourier transformation.

IV Extension of the procedure to the general case

The results we have obtained for minimal codes may be generalized to all cyclic codes, by an extension of a method suggested by Cohen, Godlewski, and Perrine [4]. We state it as:

Theorem 1: Let e_i be the period of the codemord $\underline{a}_i$ and $T^{\varphi}(\underline{a}_i)$ the codeword we get by shifting $\underline{a}_i$ cyclically φ times. Let C be a cyclic code which is a direct sum of minimal codes M_i, that is, $C = \Sigma_i M_i$. Let $\underline{a}_i \in M_i$. Then, the $\pi_i e_i$ distinct codewords

$$\Sigma_i T^{\varphi i}(\underline{a}_i), \qquad 0 \leq \varphi_i < e_i$$

are partitionned into

$$\pi_i e_i / lcm_i(e_i)$$

cycles of period $lcm_i(e_i)$, for which the words

$$\Sigma_i T^{Si}(\underline{a}_i)$$

are representatives, where $0 \leq s_i < \gcd(lcm_{j<i}(e_j),e_i)$.

Once transposed in the frequency domain, the preceding theorem becomes :

Corollary 2: Let C be the cyclic code such that $C = \Sigma_i M_i$, and let $\underline{a}_i \in M_i$. Then the $\pi_i e_i$ spectrum vectors obtained by

$$\Sigma_i \varsigma^{j(i)\varphi i}\underline{C}_i \qquad 0 \leq \varphi_i < e_i$$

where $\underline{C}_i$ is the spectrum vector of $\underline{a}_i$, and $j(i)$ a subscript of a non-zero orbit of M_i, are partitionned into

$$\pi_i e_i / lcm_i(e_i)$$

cycles of period $lcm_i(e_i)$. The frequency-domain cycle representatives are given by

$$\Sigma_i \varsigma^{j(i)Si}\underline{C}_i$$

where $0 \leq s_i < \gcd(lcm_{t<i}(e_t),e_i)$.

From this theorem and the foregoing theory, we can state the following algorithm applicable to the weight enumeration of binary cyclic codes:

Algorithm:

$$\text{Let } C = \sum_{i=1}^{r} M_i \ :$$

1. Compute the spectrum vector of the code's generator polynomial.

2. Identify the r non-zero orbits of C.
   Define :
   k(i) : number of elements of the i^{th} orbit.
   j(i) : subscript of one element of the i^{th} orbit.

3. Compute :
   3.1 β_i : element of $GF(2^m)$ "allowed" for the i^{th} orbit.
   3.2 e_i : period of the cycles of M_i.
   3.3 N_{Ci} : number of non-zero cycles in M_i.

4. Form the r-tuples $(\beta_1^{L1}, \beta_2^{L2}, \ldots, \beta_r^{Lr})$ with $L_i = -\infty, 0, 1, \ldots, N_{Ci}-1$.

   4.1 For each r-tuple, compute the characteristic r-tuples of cycle representatives :

$$R = (\varsigma^{j(1)S1}\beta_1^{L1}, \varsigma^{j(2)S2}\beta_2^{L2}, \ldots, \varsigma^{j(r)Sr}\beta_r^{Lr})$$

$$s_i = 0, 1, \ldots, \gcd(lcm_{t<i}(e_t),e_i)-1.$$

4.1.1 Compute the frequency-domain cycle representative, by application of the conjugacy constraints.

4.1.2 Compute the weight of the time-domain corresponding cycle representative, W, and add it up in the weight enumeration table :

$$A_W \leftarrow A_W + per(\underline{R}).$$

Example:

Let us take the cyclic code C(15,6), over GF(2), with generator polynomial corresponding to the codeword :

$$\underline{c} = (110011100100000).$$

1. The spectrum vector of $\underline{c}$ is

$\underline{C} = (0,0,0,0,0,\alpha^5,0,\alpha^5,0,0,\alpha^{10},\alpha^{10},0,\alpha^5,\alpha^{10})$

2. There are 2 non-zero orbits whose subscripts are respectively the elements of the cyclotomic sets { 5,10 } and { 7,11,13,14 }.

   We get k(1)=2, j(1)=5 and k(2)=4, j(2)=7.

3\.
   3.1 $\beta_1 = \alpha^5$, $\beta_2 = \alpha^1$.
   3.2 $e_1 = 3$, $e_2 = 15$.
   3.3 $N_{C1} = 1$, $N_{C2} = 1$.

4. $R = (\varsigma^{j(1)S1}\beta_1^{L1}, \varsigma^{j(2)S2}\beta_2^{L2})$

   with : $\varsigma = \alpha$,
   $s_1 = 0$
   $s_2 = 0,\ 1,\ 2$
   $L_1 = -\infty,\ 0$
   $L_2 = -\infty,\ 0$

i.e. $R = (\alpha^{5S1}\alpha^{5L1},\ \alpha^{7S2}\alpha^{L2})$

L_2	L_1	s_2	s_1	R	Cycle representative	Weight	Period
$-\infty$	$-\infty$	0	0	$(0,\ 0)$	(000000000000000)	0	1
$-\infty$	0	0	0	$(\alpha^0,\ 0)$	(011011011011011)	10	3
0	$-\infty$	0	0	$(0,\ \alpha^0)$	(000100110101111)	8	15
0	0	0	0	$(\alpha^0,\ \alpha^0)$	(011111101110100)	10	15
0	0	1	0	$(\alpha^0,\ \alpha^7)$	(111001000001100)	6	15
0	0	2	0	(α^0,α^{14})	(101010010110000)	6	15

The weight enumeration of C(15,6) is then:

$A_0 = 1$
$A_6 = 2 \times 15 = 30$
$A_8 = 1 \times 15 = 15$
$A_{10} = 1 \times 3 + 1 \times 15 = 18.$

V Conclusions

In this paper we have presented an efficient and simple procedure for the weight enumeration of cyclic codes which makes use of a Galois-Fourier transform of the codewords. Further extension is also possible by exploiting the automorphism of any binary cyclic code under the operation of squaring a codeword which yields another codeword of the same weight and period as the original one. A complete exploitation of the classes of automorphism is difficult because of the large amount of memory which is required. A partial exploitation of the procedure is however possible within the usual memory constraint and is currently being tested.

REFERENCES

[1] Goethals, J.-M., "Analysis of Weight Distribution in Binary Cyclic Codes", IEEE Transactions on Information Theory, vol IT-12, no 2, pp 401, July 1966.

[2] Willett, M. C., "Cycle Representatives for Minimal Cyclic Codes", IEEE Transactions on Information Theory, vol IT-21, no 6, pp 716-718, November 1975.

[3] Allard, P. E., Shiva, S. G. S., and Tavares, S. E., "A Note on the Decomposition of Cyclic Codes into Cyclic Classes", Information and Control, vol 22, pp 100-106.

[4] Cohen, G., Godlewski, P., et Perrine, S., "Sur les idempotents des codes", E.N.S.T., Paris.