Discrete Mathematics 56 (1985) 111–116
North-Holland

FINITE FIELD TRANSFORMS AND SYMMETRY GROUPS*

R.M. CAMPELLO de SOUZA and P.G. FARRELL

The Electrical Engineering Laboratories, University of Manchester, Manchester M13 9PL, United Kingdom

Received December 1984

Decoding methods for error-correcting codes which are based on syndrome look-up tables are of limited use due to the rapidly increasing amount of storage that they require as the number of check digits of the code increases. A method is described which uses shortened syndrome look-up tables in an efficient way, thus providing an improvement with respect to classical syndrome decoding methods. The algorithm can be characterised in general as a type of permutation decoding which uses transform domain information, with the interesting variation that permutations not preserving the code are also allowed.

1. Introduction

Fourier transforms defined over finite fields and finite rings have been investigated by many researchers [6]. Primarily, these transforms have been used in the field of digital signal processing to implement faster finite digital convolutions [7, 1]. More recently, they have been applied in the area of error control codes to produce faster encoding and decoding methods for Reed–Solomon (RS) codes [8]; also, they have been used to provide a description in the frequency (transform) domain of various types of error control code [2]. In this paper, by exploring the relations between the Galois Field Transform (GFT) and some finite groups, a simple kind of syndrome look-up table decoding algorithm for cyclic codes is presented. Such algorithms, though they can be applied to any (n, k, d) linear code, resulting in minimum decoding delay and minimum error probability, become impractical to implement for large $(n-k)$, in the sense that a large storage medium is needed. However, by proper partitioning of the set of all syndromes into equivalence classes, it is possible to reduce the required storage, therefore permitting the decoding of longer codes. This paper describes a study of such reduced storage methods.

2. The Galois field transform

The vectors $(a_i)=(a_0,\ldots,a_{n-1})$, $a_i\in \mathrm{GF}(q)$, and $(A_j)=(A_0,\ldots,A_{n-1})$, $A_j\in \mathrm{GF}(q^m)$, form a GFT pair (denoted by $(a_i)\leftrightarrow(A_j)$) if and only if

$$A_j=\sum_{i=0}^{n-1} a_i\alpha^{ji},\quad a_i=(n \bmod p)^{-1}\sum_{j=0}^{n-1} A_j\alpha^{-ji},\tag{1}$$

* Presented at the International Symposium on Algebra and Error Correcting Codes: Theory and Applications, Toulouse, June 28–30, 1983.

where p is the characteristic of GF(q), α is an element of order n of GF(q^m) and $n \mid q^m - 1$. Here we consider the case $q = 2$ and $n = 2^m - 1$. The definition of the GFT pair (1) is entirely analogous to the definition of a Discrete Fourier Transform (DFT) pair in which the kernel of the transformation $e^{-j2\pi/n}$ is substituted by α, nth root of unity in GF(q^m). The DFT has many properties which carry over into the finite field case. Among these, two are of special significance: If

$$(a_i) \leftrightarrow (A_j), \quad i, j = 0, 1, \ldots, n-1,$$

then

(i) For i_0 a constant $(0 \leqslant i_0 \leqslant n-1)$,

$$(a_{i-i_0}) \leftrightarrow (\alpha^{ji_0}A_j) \text{ (time-shift).} \tag{2}$$

(ii) For l a constant $(0 < l \leqslant n-1, (l, n) = 1)$,

$$(a_{li}) \leftrightarrow (A_{j/l}) \text{ (scaling).} \tag{3}$$

The proof of these properties follow similar lines to those for the DFT and are not presented here [3].

Also, it can be shown [2] that the components of (a_i) belong to GF(q) if and only if

$$\text{(iii)} \quad A_j^q = A_{jq}, \tag{4}$$

where indexes are considered modulo n.

3. Symmetry groups

If F is a geometrical figure in a plane or space, a symmetry of F is a bijection $f: F \rightarrow F$, which preserves distances; i.e., for all points $a, b \in F$ the distance from $f(a)$ to $f(b)$ is the same as the distance from a to b. The set of all symmetries of a geometric figure forms a group under composition because the composition and the inverse of two distance preserving compositions is also distance preserving. One example of such a group is C_n, the group of proper rotations of a regular polygon with n sides; C_n is a cyclic group of order n generated by a rotation of $2\pi/n$ radians [4].

One way of partitioning the set of n-tuples of weight t is to put them into cyclic equivalence classes, i.e., in every class the elements are cyclic shifts of one another. To find the number of orbits in such a partition, N_t, we apply Burnside's theorem [4] with the group C_n:

$$N_t = \frac{1}{|G|} \sum_{g \in G} |\text{Fix } g|, \tag{5}$$

where Fix $g=\{x\in X \mid g(x)=x\}$. For $G\equiv C_n$ (5) becomes

$$N_t=\frac{1}{n}\sum_{d\mid n}|\text{Fix } g^{n/d}|\ \Phi(d), \tag{6}$$

where $g^{n/d}$ is an element of order d of C_n and $\Phi(d)$ is the number of such elements. The expression for the total number of elements stored for a t error-correcting code of length n is then

$$N=\sum_{i=1}^{t}N_i=\frac{1}{n}\sum_{i=1}^{t}\sum_{d\mid n}|\text{Fix } g^{n/d}|\ \Phi(d), \tag{7}$$

where $\Phi(\cdot)$ is the Euler totient function.

By allowing improper rotations (reflections) to be applied to the elements of C_n we obtain a group of order $2n$ which is known as the dihedral group D_n [7]. In doing so, the positions in a vector of length n change from i to $n-1$ or $i(n-1)$ since $n-i\equiv i(n-1) \pmod n$. The above mapping is then a particular case of the mapping

$$\{0,1,\ldots,n-1\}\to\{0,1,\ldots,n-1\}$$
$$i\to li \pmod n,$$

where we assume $(l,n)=1$ guarantee weight preservation. As an example we show the partition of the 21 7-tuples of weight two, using the above permutation with $l=2$; the numbers denote the positions of the non-zero components in each 7-tuple:

$$\{01,02,03\},\{03,06,05\},\{12,24,41\},\{13,26,45\},\{15,23,46\},$$
$$\{16,25,43\},\{35,63,56\}.$$

The total number of orbits obtained is $(m=3, n=7, t=2)$

$$N=\frac{1}{m}C_n^t=\frac{21}{3}=7,$$

where $m=3$ is the multiplicative order of 2 modulo 7. The size of each orbit depends, for a given n, on the value of m, i.e., the multiplicative order of l modulo n. For instance, in the case of $n=7$ we can reduce the number of orbits to 4 by choosing, instead of $l=2$, the value of $l=3$.

4. Decoding of cyclic codes

Let $c(x)$ be a codeword of a cyclic code which is transmitted through a channel where random errors might occur. If $e(x)$ denotes the error vector, then the received vector $r(x)$ is

$$r(x)=c(x)+e(x). \tag{8}$$

The syndrome of $r(x)$ is

$$S'_j = r(\alpha^i) = e(\alpha^i), \quad j = 1, \ldots, 2t$$

so that S'_j gives $2t$ components of the transformed error vector (E_j). The decoder's task is to find the remaining $n-2t$ components. Without loss of generality,

$$S'_j = \alpha^{r'_j} \quad \text{for some } r'_j \in \{0, 1, \ldots, n-1\} \cup \{-\infty\},$$

since $n = q^m - 1$. Applying the cyclic partition defined by the group C_n to all n-typles of weight t, we use the GFT to relate the syndrome S_j of the orbit leader (OL) and the syndrome S'_j of the received vector, which we assume to be in the class defined by OL. By property (i) of the GFT

$$S'_j = \alpha^{ji_0} S_j, \quad 0 \leqslant i_0 \leqslant n-1, \quad \text{and} \quad r'_j = r_j + ji_0, \tag{9}$$

where by (iii), we consider only those values of $j \in C_j$, the cyclotomic coset modulo n over GF(2) [5]. Therefore the following set of equations can be generated:

$$\begin{aligned} r'_1 &= r_1 + i_0 \\ r'_3 &= r_3 + 3i_0 \\ r'_5 &= r_5 + 5i_0 \\ \vdots \quad & \quad \vdots \\ r'_j &= r_j + ji_0, \quad j \in C_j \end{aligned} \tag{10}$$

By direct manipulation on (10) above we can obtain the relations

$$\begin{aligned} r'_3 - 3r'_1 &= r_3 - 3r_1 \\ r'_5 - 5r'_1 &= r_5 - 5r_1 \\ \vdots \quad & \quad \vdots \\ r'_j - jr'_1 &= r_j - jr_1, \end{aligned} \tag{11}$$

which define the conditions for OL (defined by r_j) and $e(x)$ (defined by r'_j) to be in the same class. Once the class is identified, the class location is given, from (10), by

$$i_0 = r'_1 - r_1. \tag{12}$$

We can now apply property (iii) of the GFT to reduce the number of classes. The case $l = 1/2$ leads to

$$S'_j = S_{2j} = S_j^2 \quad \text{and} \quad r'_j = 2r_j. \tag{13}$$

If this is applied to every element in each of the classes defined by (11), we obtain the following decoding algorithm for cyclic codes:

(1) Calculate the syndrome $S'_j = \alpha^{r'_j}$ of the received codeword and check if (11) applies; if 'yes', find the error vector from the corresponding OL and equation (12). Otherwise:

(2) Apply (13) and check for (11) again; if a 'yes' is found, find the error vector from OL, (12) and applying the inverse of (iii) to the time domain vector; otherwise go to (2) again, etc.

Using this decoding method the (15, 7, 5) binary BCH code can be decoded by storing only 4 different syndromes instead of the set of 120 syndromes required for a full look-up table decoding method.

The permutation defined by (13) is a code preserving one. To allow non-preserving permutations we use the fact that if $p(x)=\sum_{i=0}^{n-1} a_i x^i$ is a polynomial over GF(q), and $p_\mu(x)$ is the polynomial obtained from $p(x)$ by the permutation

$$r_\mu : x^i \rightarrow x^{\mu i}, \quad (\mu, n) = 1,$$

then α^l is a root of $p(x)$ iff $\alpha^{l/\mu}$ is a root of $p_\mu(x)$. This result and property (iii) of the GFT provides a way to relate the syndromes of error vectors which are linked by a permutation that does not preserve the code. The only alteration needed in the decoding steps is to calculate the syndrome of the vector $r_{1i}(x)$, which is obtained by applying the permutation $x^i \rightarrow x^{li}$ to $r(x)$. In fact, this new syndrome is just a rearrangement of S_j, with the index j becoming $(j/l) \pmod n$. Once this rearrangement is worked out for the given l, sets of equations similar to (11) and (13) can be obtained and the decoding follows as before. A comparison involving the amount of storage required between the algorithm just described and similar methods is given in Table 1.

Table 1
Storage requirements for look-up table decoding methods

	Number of stored elements					
Type of	n	7	11	15	23	31
algorithm	t	2	4	3	3	5
standard synd. decoding		28	231	575	2047	174902
Meggitt decoder		4	21	39	89	5645
GFT-based algorithm		2	4	14	9	1130

5. Conclusions

A modified syndrome look-up table decoding algorithm for cyclic block codes has been described, which greatly reduces the number of syndromes that need to be stored. The algorithm is based on permutation decoding, but makes use of permutations which are not code-preserving. The properties of the Galois Field Transform (GFT) are used to relate the syndrome of the permuted orbit leaders to the syndrome of the received, possibly eroneous, codeword. The additional computation required to make these relations is less than comparable to the computation of the syndrome of the received word. Thus this modified syndrome look-up decoding algorithm is another useful and practical example of the application of finite field transform techniques to error-correcting codes.

Acknowledgment

R.M. Campello de Souza would like to acknowledge the partial support provided for this research by the Conselho Nacional de Desenvolvimento Cientifico e Tecnologico (CNPq).

References

[1] R.C. Agarwal and C.S. Burrus, 'Number-theoretic transforms to implement fast digital convolution', IEEE Proc. 63 (1975).
[2] R.E. Blahut, Transform techniques for error control codes, IBM J. Res. Develop. 23 (3) (1979).
[3] R.N. Bracewell, The Fourier Transform and its Applications (McGraw-Hill, New York, 1978).
[4] W.J. Gilbert, Modern Algebra with Applications (Wiley, New York, 1976).
[5] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).
[6] J.M. Pollard, The fast Fourier transform in a finite field, Math. Comp. 25 (114) (1974).
[7] C.M. Rader, Discrete convolutions via Mersenne transforms, IEEE Trans. Comput. 21 (1972).
[8] I.S. Reed, T.K. Truong and L.R. Welch, The fast decoding of RS codes using Fermat transforms, IEEE Trans. Inform. Theory (1978).