22

Reprinted from INFORMATION AND CONTROL
All Rights Reserved by Academic Press, New York and London

Vol. 40, No. 3, March 1979
Printed in Belgium

Fourier Transform over Finite Groups for Error Detection and Error Correction in Computation Channels

M. G. KARPOVSKY AND E. A. TRACHTENBERG

Tel-Aviv University, Ramat-Aviv, Tel-Aviv, Israel
and State University of New York at Binghamton, N.Y., U.S.A.

We consider the methods of error detection and correction in devices and programs calculating functions $f\colon G \to K$ where G is a finite group and K is a field. For error detection and correction we use linear checks generated by convolutions in the field K of the original function f and some checking idempotent function $\delta\colon G \to \{0, 1\}$. For the construction of the optimal checking function δ we use methods of harmonic analysis over the group G in the field K. Since these methods will be the main tools for the construction of optimal checks, we consider the algorithms for the fast computation of Fourier Transforms over the group G in the field K. We solve the problem of error detecting and correcting capability for our methods for two important classes of decoding procedures (memoryless and memory-aided decoding) and consider the question of syndrome computation for these methods. We describe also properties of error correcting codes generated by convolution checks.

1. STATEMENT OF PROBLEM

Development of universal methods for detecting and correcting errors in the process of calculation of the given function realized with the aid of specific devices, or with the aid of computer programs is a topical problem. The present study, devoted to a possible solution of this problem, deals with the detection and correction of errors in calculation of functions defined over finite groups (commutative and non-commutative), an "error" in this context being defined as catastrophic failure of the calculating device, or as an error in the text of the program.

Examples of the devices in question are: blocks of arithmetic units of a computer, networks whose operation is described by two or many-valued switching functions, linear control systems over finite groups (Karpovsky and Trachtenberg, 1977a), rearrangeable switching networks whose output depends on permutation of input terminals (Opferman and Tsao-Wu, 1971), etc. We shall refer to any device or program calculating the given f as a computation channel f.

Let f be a function defined over a finite group G of order $|G|$ and $\{K_j\}$, $(j = 1,..., m)$ be a set of fields, such that $\operatorname{Im} f \subseteq \bigcap_{j=1}^{m} K_j$ (Im f is the range of f).

0019-9958/79/030335-24$02.00/0

For detecting and correcting errors in channel f, we shall use systems of linear checks in the fields K_j:

$$(\delta_{H_j} \circledast f)(t) \triangleq \sum_{\zeta \in G} \delta_{H_j}(\zeta) f(t \odot \zeta^{-1}) = \varphi_j(t) + \lambda_j\,, \ (K_j), \tag{1}$$

for all $t \in G$, $j = 1,..., m$. Where $\circledast$ is the operation of group convolution, $\odot$ is the group operation, ζ^{-1} is the inverse of $\zeta \in G$,

$$\delta_{H_j}(\zeta) = \begin{cases} 1, & \zeta \in H_j; \\ 0, & \zeta \notin H_j; \end{cases} \qquad (H_j \subseteq G)$$

φ_j: $G \to K_j$ some "simple" checking function (for example, $\varphi_j = \text{const}$).

All arithmetic operations in (1) are carried out in the field K_j, as indicated by the symbol (K_j) on the right.

Methods of error detection and error correction in computation channels by means of linear checks of type (1) were considered by Karpovsky (1977a) for the case when G is an Abelian group, $m = 1$ and $K_1 = C$ — the field of complex numbers and in (Karpovsky and Trachtenberg, 1977b) were given some results (without proofs) about error detection and correction in computation channels for the case $K_1 = K_1 = \cdots = K_m = C$. Several examples of linear checks of type (1) for such important computation channels as counters, adders, subtractors, multipliers, etc. were given by Karpovsky (1977a) and Karpovsky and Trachtenberg (1977b).

We note that for the important case $\operatorname{Im} f \subset N$ (N is the set of integers) the transition, in (1), from the field C of complex numbers to the field $GF(q)$ of q elements ($q > \max_{t \in G} f(t)$, q being a prime number) results, generally speaking, in reduction of the complexity $\| \delta_{H_j} \| \triangleq \sum_{\zeta \in G} \delta_{H_j}(\zeta)$ of check (1) (see Section 4).

We shall also consider in this paper, methods of error detection and correction for system of functions defined on finite groups (Section 4) and methods of network implementation of these checks (Section 5).

In searching for optimal checks of type (1) in terms of $\| \delta_{H_j} \|$, we shall apply methods of harmonic analysis over group G in the fields K_j ($j = 1,..., m$). (The choice of $\| \delta_{H_j} \|$ as complexity criterion in (1) will be justified in Section 5.) An analogous approach, based on methods of harmonic analysis over finite groups, is described by Karpovsky (1976, 1977b).

Since harmonic analysis over finite group G in the field K will be the main tool in this work we shall consider in Section 3 the algorithms of fast computation of Fourier transforms for functions f: $G \to K$.

Methods of harmonic analysis yield simple and convenient from the computation viewpoint search procedures for optimal checks, but on the other hand have the following basic disadvantages:

(i) For a given finite group, it is not in every field K that technique of Fourier transform may be used.

(ii) Only checks where H_j are normal subgroups of G will be constructed.

It should also be noted that checks of type 1, at $\varphi_j(t) = 0$ for all $t \in G$, $\lambda_j = 0$ and $K_j = GF(q)$ $(j = 1,..., m)$, are analogous to those used for syndrome calculation in decoding procedure for q-ary linear error-correcting codes. The properties of error-correcting codes generated by systems of checks of type (1) will be considered in Section 7.

In addition to the present section, the paper contains six others:

The second section presents some prerequisites from harmonic analysis over finite group G in a field K. The third section presents algorithms for the fast computation of the corresponding Fourier transforms when G is a direct product of some groups H_j, $G = \prod_{j=1}^{n} H_j$. The fourth section deals with construction methods for optimal checks of type (1). The fifth section deals with calculation of error syndromes. The theorems of the sixth section solve the problem of the correcting and detecting capability of systems of checks (1) for two different methods of decoding. Section 7 is devoted to linear error-correcting codes generated by a system of checks of type (1).

2. Fourier Transforms over the Finite Group G and Field K

Let G be an arbitrary finite group with $|G|$ elements and K any field of characteristic char K. In the space $L_{G,K} = \{f : G \to K\}$ we shall use the elements of the non-equivalent absolutely irreducible representations of G over the field K as an orthogonal basis.

Recall (Dornhoff, 1971) that representation ω of degree d_ω in a linear space V (dim $V = d_\omega$) over K is defined as a homomorphism ω: $G \to GL(d_\omega, K)$, where $GL(d_\omega, K)$ is the group of all invertible $(d_\omega \times d_\omega)$-matrices over K. The value of representation ω at the point $t \in G$ will be denoted by $[\omega, t]$ and the functions generated by $[\omega, t]$ when ω and t are fixed will be denoted by $[\omega, \cdot]$ and $[\cdot, t]$ respectively.

Two representations ω_1 and ω_2 of the same degree $d_{\omega_1} = d_{\omega_2}$ are said to be equivalent if there exists an invertible $(d_{\omega_1} \times d_{\omega_1})$-matrix Q over K such that $Q^{-1}[\omega_1, t]Q = [\omega_2, t]$, (K) for every $t \in G$.

A representation ω in linear space V over K is said to be irreducible if V has no proper ω-invariant subspaces, and is absolutely irreducible if it remains irreducible in any extension of K.

Henceforth it will be assumed that

(i) char $K = 0$, or char K does not divide $|G|$. (Throughout this paper, $|A|$ denotes the cardinality of the set A, and $a \mid b$ $(a \times b)$ signifies that a is (not) a divisor of b.)

(ii) K is such that if ω is an irreducible representation of G in a linear space V over K, then ω is absolutely irreducible (i.e., K is the so-called splitting field for G. See, e.g., Dornhoff, 1974).

We note that $K = C$ (C, the field of complex numbers) is the splitting field for any G. Conditions for K to be a splitting field for a given group G, and construction methods for absolutely irreducible representations of G in K, are considered in algebraical literature for the great variety of groups G and fields K (see, e.g., Dornhoff, 1971).

Let $\hat{G} = \{\omega\}$ denote the set of all nonequivalent absolutely irreducible representations of G in K, indexed so that ω is of degree d_ω ($\hat{G}$ is the dual object for G); $|\hat{G}|$ equals the number of conjugate classes of G, and we have

$$\sum_{\omega \in \hat{G}} d_\omega^2 = |G|. \tag{2}$$

Let $f_i: G \to M(a_i, K)$ where $M(a_i, K)$—the set of all $(a_i \times a_i)$—matrices over K and $\hat{\varphi}_i: \hat{G} \to M(b_i d_\omega, K)$ where for every $\omega \in \hat{G}$ $\hat{\varphi}_i(\omega)$ is a $(d_\omega \times d_\omega)$-block matrix over K with blocks

$$\hat{\varphi}_i^{(j,s)}(\omega) \in M(b_i, K) \qquad (i = 1, 2; j, s = 1,..., d\omega).$$

Denote

$$\langle f_1, f_2 \rangle_G \triangleq \sum_{t \in G} (f_1(t) \otimes f_2(t^{-1}));$$

$$\langle \hat{\varphi}_1, \hat{\varphi}_2 \rangle_G \triangleq \sum_{\omega \in \hat{G}} \sum_{j,s=1}^{d\omega} (\hat{\varphi}_1^{(j,s)}(\omega) \otimes \hat{\varphi}_2^{(s,j)}(\omega)). \qquad (K). \tag{3}$$

Here $\otimes$ Kronecker product of matrices;

$$\langle f_1, f_2 \rangle_G \in M(a_1 a_2, K); \qquad \langle \hat{\varphi}_1, \hat{\varphi}_2 \rangle_G \in M(b_1 b_2, K).$$

Let $[\omega, t]_{i,j}$ denote (i, j)-th element of matrix $[\omega, t]$ $(i, j = 1,..., d_\omega)$. We recall (Dornhoff, 1971) the orthogonality relations for the $|G|$ functions $\{[\omega, \cdot]_{i,j}\}$

$$\langle [\omega_1, \cdot]_{i_1,j_1}, [\omega_2, \cdot]_{i_2,j_2} \rangle_G = \frac{|G|}{d_{\omega_1}} \delta_{\omega_1,\omega_2} \delta_{i_1,i_2} \delta_{j_1,j_2}; \quad (K) \tag{4}$$

(Here $\omega_1, \omega_2 \in \hat{G}$; $i_1, j_1 = 1,..., d_{\omega_1}$; $i_2, j_2 = 1,..., d_{\omega_2}$; δ is the Kronecker delta, and $|G|/d_\omega \in K$.)

The character of the representation ω is defined as the trace $[\omega, \cdot]$. The characters satisfy the following orthogonality relations

$$\langle \text{trace}\, [\omega_1, \cdot], \text{trace}\, [\omega_2, \cdot] \rangle_G = |G| \delta_{\omega_1,\omega_2};$$

$$\langle \text{trace}\, [\cdot, t_1], \text{trace}\, [\cdot, t_2^{-1}] \rangle_G = \frac{|G|}{\nu_{t_1}} \delta_{t_1,t_2}; \qquad (K)$$

where ν_{t_1} is the cardinality of the conjugate class of G which contains t_1 (Dornhoff, 1971).

We consider now the important case of Abelian group G and Galois field $K = GF(q^r)$. In this case G may be represented as a direct product of cyclic subgroups

$$G = H_1 \times \cdots \times H_n , \text{ i.e. } t \in G,\ t = (t_1 ,\dots, t_n),\ t_j \in \{0, 1,\dots, | H_j | - 1\},$$

$| H_j |$ is a power of a prime number, the group operation is componentwise addition mod $| H_j |, j = 1,\dots, n$. Let μ be the least common multiple of $| H_1 |,\dots, | H_n |$ and $\sqrt[\mu]{1} \in GF(q^r)$, i.e. the equation $x^\mu = 1$ is solvable in $GF(q^r)$ or, in other words, $\mu \mid q^r - 1$. Since $\mu \mid | G |$ then $q \nmid | G |$ and $GF(q^r)$ is a splitting field for G. In this case $d_\omega = 1$ for all $\omega \in \hat{G}$, $\hat{G} = \mathscr{P}_1 \times \cdots \times \mathscr{P}_n$, $\hat{G}$ is a multiplicative group of characters which is isomorphic to G and H_j isomorphic to $\mathscr{P}_j$, i.e., $\omega = (\omega_1 ,\dots, \omega_n)$, $\omega_j \in \{0, 1,\dots, | H_j | - 1\}$ and we have

$$[\omega, t] = \prod_{j=1}^{n} \xi_j^{\omega_j t_j},\ \omega_j , t_j \in \{0, 1,\dots, | H_j | - 1\}, (GF(q^r)). \tag{5}$$

Here $\xi_j = \sqrt[|H_j|]{1} \in GF(q^r)$ $(j = 1,\dots, n)$.

For the case $K = C$, $\xi_j = \exp(2\pi i/| H_j |)$, $i = (-1)^{1/2}$ and if $| H_1 | = \cdots = | H_n |$ then, $[\omega, \cdot]$ is known as Chrestenson functions and for $q = 2$ as Walsh functions (see, e.g., Karpovsky, 1976).

Let $f: G \to K$. It follows by (3), (4) that the Fourier transforms $F_{G,K}: f \to \hat{f}$ and inverse Fourier transforms $F_{G,K}^{-1}: \hat{f} \to f$ on the group G in the field K may be defined as follows

$$\hat{f}(\omega) = \frac{d_\omega}{| G |} \langle f, [\omega, \cdot]\rangle_G , \tag{6}$$

$$f(t) = \langle \hat{f}, [\cdot, t]\rangle_{\hat{G}} . \tag{7}$$

For the Fourier transform $F_{G,K}: f \to \hat{f}$ on the group G in the field K the usual properties of linearity, translation of arguments, convolution, Plancherel, Wiener-Khinchine, Poisson theorems are valid.

Now let $\Omega \subseteq \hat{G}$ and denote

$$\Omega^\perp \triangleq \bigcap_{\omega\in\Omega} \operatorname{kern} \omega = \bigcap_{\omega\in\Omega} \{t \mid [\omega, t] = E\}, E\text{-the identity matrix.}$$

A subset $\Omega \subset \hat{G}$ is said to be closed (notation $\Omega = \bar{\Omega}$) if for any $\omega \notin \Omega$ we have $\Omega^\perp \not\subset \operatorname{Kern} \omega$. Then for every normal subgroup H of G there is a unique $\bar{\Omega} \subseteq \hat{G}$ such that $\bar{\Omega}^\perp = H$. Moreover, any $\bar{\Omega}$ is isomorphic to the dual object $\widehat{G/\bar{\Omega}^\perp}$ of the factor group $G/\bar{\Omega}^\perp$ and elements of the set $\bar{\Omega}$ are constants on the cosets of G modulo $\bar{\Omega}^\perp$; in addition if $\alpha(\bar{\Omega}) \triangleq \sum_{\omega\in\Omega} d_\omega^2$ then $\alpha(\bar{\Omega}) \mid | G |$, $\alpha(\hat{G}) = | G |$ and $\alpha(\bar{\Omega}) \, | \bar{\Omega}^\perp | = | G |$.

EXAMPLE 1. Let $f(t) = t^2 - 170t - 35$, $t \in \{0,\dots, 2^8 - 1\}$ and t represented

TABLE I

$G = C_2 \times S_3$			$\hat{G} = \hat{C}_2 \times \hat{S}_3$							
t, τ	(t_1, t_2)	t	0	1	2	3	4	5	f_1	f_2
0	(0, 0)	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	1	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	0	10
1	(0, (132))	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}$	1	1	1	1	$\begin{pmatrix} 5 & 8 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 8 \\ 3 & 5 \end{pmatrix}$	0	1
2	(0, (123))	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$	1	1	1	1	$\begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix}$	1	0
3	(0, (12))	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	1	1	10	10	$\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$	0	4
4	(0, (13))	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	1	1	10	10	$\begin{pmatrix} 5 & 8 \\ 8 & 6 \end{pmatrix}$	$\begin{pmatrix} 5 & 8 \\ 8 & 6 \end{pmatrix}$	1	0
5	(0, (23))	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$	1	1	10	10	$\begin{pmatrix} 5 & 3 \\ 3 & 6 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 \\ 3 & 6 \end{pmatrix}$	0	0
6	(1, 0)	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	10	1	10	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}$	0	2
7	(1, (132))	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}$	1	10	1	10	$\begin{pmatrix} 5 & 8 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 6 & 3 \\ 8 & 6 \end{pmatrix}$	0	0
8	(1, (123))	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$	1	10	1	10	$\begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix}$	$\begin{pmatrix} 6 & 8 \\ 3 & 6 \end{pmatrix}$	1	1
9	(1, (12))	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	1	10	10	1	$\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$	$\begin{pmatrix} 10 & 0 \\ 30 & 1 \end{pmatrix}$	0	8
10	(1, (13))	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	1	10	10	1	$\begin{pmatrix} 5 & 8 \\ 8 & 6 \end{pmatrix}$	$\begin{pmatrix} 6 & 3 \\ 3 & 5 \end{pmatrix}$	1	3
11	(1, (23))	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$	1	10	10	1	$\begin{pmatrix} 5 & 3 \\ 3 & 6 \end{pmatrix}$	$\begin{pmatrix} 6 & 8 \\ 8 & 5 \end{pmatrix}$	0	1

in the binary form $t = (t_1, \ldots, t_8)$, $t_j \in \{0, 1\}$. Then $f\colon C_2^8 \to C$ where C_2^8 is the group of binary vectors with eight components, and the group operation is componentwise addition mod 2.

All the representations of C_2^8 in C have degree one, and in a according with (5)

$$[\omega, t] = \exp\left(\pi(-1)^{1/2} \sum_{j=1}^{8} \omega_j t_j\right) = (-1)^{\sum_{j=1}^{8} \omega_j t_j}; \ \omega_j, t_j \in \{0, 1\}.$$

Fourier (Walsh) transform in this case defined by formula

$$f(\omega) = 2^{-8} \sum_{t \in C_2^8} f(t)(-1)^{\sum_{j=1}^{8} \omega_j t_j}$$

For the polynomial $f(t) = t^2 - 170t - 35$ we have $\hat{f}(\omega) = 0$ if $\| \omega \| = \sum_{j=1}^{8} \omega_j > 2$.

The dual object $\widehat{C_2^8}$ is isomorphic to C_2^8 and $\Omega = \bar{\Omega} \subseteq \widehat{C_2^8}$ iff $\bar{\Omega}$ is a subgroup of C_2^8.

Linear checks of type (1) for this polynomial will be constructed in Section 4, and error-detecting and correcting capabilities of these checks will be considered in Section 6.

EXAMPLE 2. Let G be the multiplication group of the twelve (3×3)-matrices $t = (t_{i,j})$, $i, j = 1, 2, 3$ over the field C represented in Table I. Note that G is isomorphic to the direct product of the cyclic group $C_2 = \{0, 1\}$ of order 2 with generating element 1 and the symmetric group of permutations $S_3 = \{0, (132), (123), (12), (13), (23)\}$ (see Table I). Table I lists also all absolutely irreducible representations for the given group $G = C_2 \times S_3$ in $GF(11)$ ($GF(11)$ is a splitting field for $C_2 \times S_3$.)

All closed subsets $\bar{\Omega} \subseteq \hat{G}$ with the corresponding $\alpha(\bar{\Omega})$ and $\bar{\Omega}^{\perp}$ are represented for the given group $G = C_2 \times S_3$ in Table II.

TABLE II

	Ω	$\alpha(\Omega)$	$\Omega^{\perp}$
Ω_0	{0}	1	{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
Ω_1	{0, 1}	2	{0, 1, 2, 3, 4, 5}
Ω_2	{0, 2}	2	{0, 1, 2, 6, 7, 8}
Ω_3	{0, 3}	2	{0, 1, 2, 9, 10, 11}
Ω_4	{0, 1, 2, 3}	4	{0, 1, 2}
Ω_5	{0, 2, 4}	6	{0, 6}
Ω_6	{0, 1, 2, 3, 4, 5}	12	{0}

3. Computation of Fourier Transforms for Finite Group G and Field K

We consider methods of computation of Fourier $F_{G,K}$ and inverse Fourier $F_{G,K}^{-1}$ transforms. For the case when G is a group of binary (q-ary) n-vectors, the Fourier transform on G in the field C of complex numbers is called the Walsh-Hadamard (Chrestenson-Hadamard) transform. In such cases, there exist algorithms of the Fast Walsh-Hadamard (Chrestenson-Hadamard) transforms, which require $n \cdot 2^n$ $(n \cdot q^n)$ elementary operations, and $2^n(q^n)$ memory cells to compute $F_{G,C}$ or $F_{G,C}^{-1}$. Those algorithms are generalized for the case where G is an arbitrary finite Abelian group and $K = C$ in (Apple and Wintz, 1971). In (Karpovsky, 1977c) these algorithms were given for G and arbitrary (non-Abelian) finite group and $K = C$. We generalize (see Theorem 1) this technique for the case where G finite group isomorphic to a direct product of some groups H_j $(j = 1,..., n)$, $G = \prod_{j=1}^{n} H_j$ and K is an arbitrary field (such that char $K = 0$ or char $K \nmid |G|$ and K is a splitting field for G).

For this case (see, e.g., Dornhoff, 1971)

$$[\omega, t] = \bigotimes_{j=1}^{n} [\omega_j , t_j], (K). \tag{8}$$

where $\omega_j \in H_j$, $t_j \in H_j$, and $\otimes$ denotes the Kronecker product of matrices over K.

Theorem 1. *Let $G = \prod_{j=1}^{n} H_j$. For any $f: G \to K$ set $f = f^{(n)}$ $\hat{f} = \hat{f}^{(n)}$ and for any $\omega = (\omega_1 ,..., \omega_n)$ denote by $(\hat{f}^{(n)})_p (\omega_1 ,..., \omega_n)$ the $(d_{\omega_n} \times d_{\omega_n})$-block matrix received by partitioning of $\hat{f}^{(n)}(\omega_1 ,..., \omega_n)$ with blocks of dimensions $(\prod_{r=1}^{n-1} d_{\omega_r} \times \prod_{r=1}^{n-1} d_{\omega_k})$.*

Let

$$f^{(j-1)} = \langle f^{(j)}, [\omega_j , \cdot]\rangle_{H_j} , \tag{9}$$

$$\hat{f}^{(j-1)} = \langle(\hat{f}^{(j)})_p , [\cdot, t_j]\rangle_{\hat{H}_j} \qquad (j = n, n-1,..., 1). \tag{10}$$

(Here $(\hat{f}^{(j)})_p$ $(\omega_1 ,..., \omega_j , t_{j+1} ,..., t_n)$ is a $(d_{\omega_j} \times d_{\omega_j})$-block matrix received by partitioning of $\hat{f}^{(j)}(\omega_1 ,..., \omega_j , t_{j+1} ,..., t_n)$ with block of dimensions $(\prod_{r=1}^{j-1} d_{\omega_r} \times \prod_{r=1}^{j-1} d_{\omega_r})$. Then

$$\hat{f}(\omega) = \frac{d_\omega}{|G|} f^{(0)}(\omega), f(t) = f^{(0)}(t), (K). \tag{11}$$

Proof. By (3), (6), (8) we have for any $\omega \in \hat{G}$ and any $t \in G$

$$\hat{f}(\omega) = \frac{d_\omega}{|G|} \langle f, [\omega, \cdot]\rangle_G = \frac{d_\omega}{|G|} \left\langle f, \bigotimes_{j=1}^{n} [\omega_j , t_j]\right\rangle_G$$

$$= \frac{d_\omega}{|G|} \langle \cdots \langle\langle f, [\omega_n , \cdot]\rangle_{H_n} , [\omega_{n-1} , \cdot]\rangle_{H_{n-1}} ,...; [\omega_1 , \cdot]\rangle_{H_1} , (K)$$

and in view of (9) $\hat{f}(\omega) = d_\omega / |G| f^{(0)}(\omega)$, (K). Similarly, in view of (3), (7), (8) we have

$$f(t) = \langle \hat{f}, [\cdot, t] \rangle_G = \Big\langle \hat{f}, \bigotimes_{j=1}^{n} [\cdot, t_j] \Big\rangle_G$$

$$= \langle \cdots (\langle (\langle (\langle (\hat{f}^{(n)})_p, [\cdot, t_n] \rangle_{\hat{H}_n})_p, [\cdot, t_{n-1}] \rangle_{\hat{H}_{n-1}})_p \cdots [\cdot, t_1] \rangle_{\hat{H}_1}.$$

Hence, by (10), we have $f(t) = \hat{f}^{(0)}(t)$.

It follows from (9), (10) in view of (2) that each of the functions $f^{(j-1)}, \hat{f}^{(j-1)}$ $(j = n, n-1, \ldots, 1)$ is defined at $|G| = \prod_{j=1}^{n} |H_j|$ points and the number of memory cells for storage $f^{(j-1)}$ or $\hat{f}^{(j-1)}$ equals $|G|$. For computation of any specific value of $f^{(j-1)}$ or $\hat{f}^{(j-1)}$ we need $|H_j|$ multiplications. Consequently, the total number of multiplications for computing f or $\hat{f}$ by Theorem 1 equals $|G| \sum_{j=1}^{n} |H_j|$.

4. Construction of Optimal Checks

The number $\| \delta_H \|$ of nonzero values of δ_H for the check $\delta_H \circledast f = \varphi + \lambda(K)(f, \varphi\colon G \to K,\ \delta_H\colon G \to \{0, 1\}, \lambda \in K)$ affects the number of additions needed for checking the given f when f is calculated by a computer program, and affects the network complexity when f is realized by a network (see Section 5). Accordingly, we use the $\| \delta_H \|$ as a complexity criterion for the function δ_H. Let, for the given $f\colon G \to K$ and any $\gamma \in K$, $\tau \in G$,

$$\Omega_f(\gamma, \tau) \triangleq \left\{ \omega \mid \hat{f}(\omega) = \frac{d_\omega}{|G|} \gamma[\omega, \tau] \right\} \cup \{0\}, (K), \tag{12}$$

where $[0, t] = 1$ for all $t \in G$.

Theorem 2. *Let* $f\colon G \to K$, *K be any splitting field for G with* char $K = 0$ *or* char $K \nmid |G|$. *Then*

$$(\delta_{\Omega^\perp} \circledast f)(t) = \gamma \delta_{\Omega^\perp}(t \odot \tau) + \frac{|\Omega^\perp|}{|G|} \Big(\sum_{\zeta \in G} f(\zeta) - \gamma \Big), (K) \text{ for all } t \in G \tag{13}$$

iff $\bar{\Omega} \subseteq \Omega_f(\gamma, \tau)$.

Proof. Let $\bar{\Omega}^\perp$ be a normal subgroup in G. We first prove that if

$$\delta_{\Omega^\perp}(t) = \begin{cases} 1, & t \in \bar{\Omega}^\perp; \\ 0, & t \notin \bar{\Omega}^\perp; \end{cases} \tag{14}$$

then

$$\delta_{\bar{\Omega}^{\perp}}(\omega) = \begin{cases} \dfrac{d_\omega}{|G|} \, |\bar{\Omega}^{\perp}| \, E, & \omega \in \bar{\Omega}; \\ 0, & \omega \notin \Omega; \end{cases} \quad (K) \tag{15}$$

(0 is $(d_\omega \times d_\omega)$-zero matrix).

By (6)

$$\delta_{\bar{\Omega}^{\perp}}(\omega) = \frac{d_\omega}{|G|} \sum_{t \in \Omega^{\perp}} [\omega, t^{-1}], (K). \tag{16}$$

If $\omega \in \bar{\Omega}$, then $\delta_{\bar{\Omega}^{\perp}}(\omega) = d_\omega / |G| \, |\bar{\Omega}^{\perp}| \, E$, (K). If $\omega \notin \bar{\Omega}$, then $\omega \neq 0$ since $0 \in \bar{\Omega}$ for every $\bar{\Omega} \subseteq \hat{G}$. Hence, by (3), (4) for $\omega \notin \bar{\Omega}$

$$\delta_{\bar{\Omega}^{\perp}}(\omega) = \frac{d_\omega}{|G|} \sum_{t \in \bar{\Omega}^{\perp}} [\omega, t^{-1}] = \frac{d_\omega}{|G|} \sum_{t \in \bar{\Omega}^{\perp}} [\omega, t^{-1}][0, t] = 0, (K).$$

From (13) and (15) by the theorems of convolution and translation or arguments for Fourier transform $f_{G,K}$ we have for any $\omega \in \bar{\Omega}$

$$f(\omega) = \begin{cases} \dfrac{1}{|G|} \sum_{\zeta \in G} f(\zeta), & \omega = 0; \\ \gamma \dfrac{d\omega}{|G|} [\omega, \tau], & \omega \neq 0; \end{cases} \tag{17}$$

and by (17) in a view of definition (12) we have $\bar{\Omega} \subseteq \Omega_f(\gamma, \tau)$. Conversely, if $\bar{\Omega} \subseteq \Omega_f(\gamma, \tau)$, then (17) is satisfied for any $\omega \in \bar{\Omega}$ and (13) is also satisfied.

It will be shown in the next section that the complexity of a network implementation of a check (13) for the given channel $f: G \to K$ depends only on the complexity $\| \delta_H \| = \sum_{\zeta \in G} \delta_H(\zeta)$ of the function $\delta_H: G \to \{0, 1\}$.

Thus, by Theorem 2 we have the following procedure for construction of the best checking equation (13).

1. For the given $f: G \to K$, compute by (6) or by (9), (11) f.

2. By (12), construct the sets $\Omega_f(\gamma, \tau)$.

3. For the given group G, construct all closed subsets $\bar{\Omega}$ of the dual object $\hat{G}$.

4. Find $\gamma_{\mathrm{opt}} \in K$, $\tau_{\mathrm{opt}} \in G$, $\bar{\Omega}_{\mathrm{opt}} \subseteq \hat{G}$ from the condition

$$\max_{\gamma, \tau} \max_{\bar{\Omega} \subseteq \Omega_f(\gamma, \tau)} \alpha(\bar{\Omega}) \triangleq \max_{\bar{\Omega} \subseteq \Omega_f(\gamma_{\mathrm{opt}}, \tau_{\mathrm{opt}})} \alpha(\bar{\Omega}) \triangleq \alpha(\bar{\Omega}_{\mathrm{opt}}) \tag{18}$$

$$\left(\alpha(\bar{\Omega}) = \sum_{\omega \in \Omega} d_\omega^{\,2} = \frac{|G|}{|\bar{\Omega}^{\perp}|} \right).$$

5. Construct $\delta_{\bar{\Omega}^{\perp}}: G \to \{0, 1\}$ by (14), for $\gamma = \gamma_{\mathrm{opt}}$, $\tau = \tau_{\mathrm{opt}}$, $\bar{\Omega} = \bar{\Omega}_{\mathrm{opt}}$.

We note that for any f, γ, τ the set $\Omega_f(\gamma, \tau)$ depends on K. Consequently, the set $\bar{\Omega}_{\text{opt}}$ also depends on K. This poses and apparently quire difficult problem: optimal selection of a field K minimizing the complexity of the check.

We note also that if $\mathrm{Im}\, f\, C'N$ then transition from C to any field $GF(q)$ (q — a prime and $q > \max_x f(x)$) may result only in the increasing of $|\Omega_f(\gamma, \tau)|$ for all γ, τ. Consequently, $\alpha(\bar{\Omega}_{\text{opt}})$, generally speaking, increases and the complexity of the check is reduced..(See definition of $\alpha(\bar{\Omega})$ and $\bar{\Omega}^{\perp}$ in Section 2 and (14). See also Example 5.)

EXAMPLE 3. Let $f_1: C_2 \times C_3 \rightarrow GF(11)$ is defined by Table I. (see also Example 2; absolutely irreducible representations of $C_2 \times C_3$ in $GF(11)$ are given in Table I; closed subsets $\bar{\Omega} \subseteq \widehat{C_2 \times S_3}$, $\alpha(\bar{\Omega})$ and $\bar{\Omega}^{\perp}$ are represented for $C_2 \times S_3$ in Table II.)

We will find now by Theorem 2 the optimal checking equation for f_1. Table III lists the Fourier transform $\hat{f}_1(\omega)$ in $GF(11)$ clmputed by (6). Then for every $\tau \in G$

$$\Omega_{f_1}(\gamma, \tau) = \begin{cases} \{0, 1, 2, 3, 5\}, & \text{if } \gamma = 0; \\ \{0\}, & \text{if } \gamma \neq 0. \end{cases}$$

By (18)

$$\gamma_{\text{opt}} = 0; \qquad \bar{\Omega}_{\text{opt}} = \bar{\Omega}_4 = \{0, 1, 2, 3\}; \qquad \bar{\Omega}_{\text{opt}}^{\perp} = \{0, 1, 2\}.$$

Since for our group $1^{-1} = 2$, $2^{-1} = 1$ we have by (13) the following checking equation for f_1

$$f_1(t) + f_1(t \odot 1) + f_1(t \odot 2) = 1, \ (GF(11), \text{ for}$$

and $t \in G$.

We now apply Theorem 2 in the important case of pseudoboolean channels. By "pseudoboolean channel" we mean any device or any program calculating a function from n binary arguments. For this case, $G = C_2{}^n$ is a group of binary n-vectors with componentwise addition mod 2.

If K is a finite field, the necessary and sufficient condition for existence of absolutely irreducible representations of $C_2{}^n$ in K is that $|K|$ be odd. The Fourier transform in this case is known as the Walsh-Galois transform and in the case $K = C$ as the Walsh-Hadamard transform (Karpovsky, 1976).

We denote for pseudoboolean channels

$$\Omega_f(\gamma) \triangleq \{\omega \mid \hat{f}(\omega) = \gamma 2^{-n}\} \cup \{0\}. \tag{19}$$

Then, since for pseudoboolean channels $\alpha(\bar{\Omega}) = |\bar{\Omega}|$ instead of (18), we have for $\bar{\Omega}_{\text{opt}}$

$$\max_{\gamma \in R} \max_{\Omega \subseteq \Omega_f(\gamma)} |\Omega| = \max_{\Omega \subseteq \Omega_f(\gamma_{\text{opt}})} |\bar{\Omega}| = |\bar{\Omega}_{\text{opt}}|. \tag{20}$$

TABLE III

ω	(ω_1, ω_2)	$f_1(\omega)$	$f_2(\omega)$, $(GF(11))$	$f_2(\omega)$, (C)
0	(0, 0)	4	8	$\frac{5}{2}$
1	(1, 0)	0	0	0
2	(0, 1)	0	9	$-\frac{1}{6}$
3	(1, 1)	0	5	$\frac{4}{3}$
4	(0, 2)	$\begin{pmatrix}7 & 9\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}9 & 10\\ 10 & 2\end{pmatrix}$	$\frac{1}{6}\begin{pmatrix}21 & -\sqrt{3}\\ -\sqrt{3} & 1\end{pmatrix}$
5	(1, 2)	$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 0 & 9\end{pmatrix}$	$\frac{1}{6}\begin{pmatrix}6 & 2\sqrt{3}\\ 0 & 10\end{pmatrix}$

To simplify this procedure we may replace γ_{opt} and $\bar{\Omega}_{\text{opt}}$ by γ'_{opt} and $\bar{\Omega}'_{\text{opt}}$ where

$$\max_{\gamma} |\,\Omega_f(\gamma)| = \Omega_f(\gamma'_{\text{opt}}) \qquad \text{and} \qquad \max_{\bar{\Omega}\subseteq\Omega_f(\gamma'_{\text{opt}})} |\,\bar{\Omega}\,| = |\,\bar{\Omega}'_{\text{opt}}\,|. \tag{21}$$

(Note that the complexity of the check constructed by (21) is, generally speaking, higher than that of the check constructed by (20).)

EXAMPLE 4. For the pseudoboolean channel $f(t) = t^2 - 170 - 35$, f: $C_2^{\,8} \to C$ from the Example I we have $\hat{f}(\omega) = 0, \|\,\omega\,\| = \sum_{j=1}^{8} \omega_j > 2, |\,\Omega_f(0)| =$ $2^8 - \binom{8}{0} - \binom{1}{8} - \binom{8}{2} = 219$, $\gamma'_{\text{opt}} = 0$ and $\bar{\Omega}$ may be chosen as a linear space over $GF(2)$ with basis {(1100 1000), (01100100), (00110010), (10010001)}. Then $H_1 \triangleq \bar{\Omega}^{\perp}$ is a linear space with basis {(10001001), (0100 1100), (00100110), (0001 0011)}. Since the for every $t \in C_2^{\,8}$ $t = t^{-1}$, we have by (13) for $f(t) =$ $t^2 - 170t - 35$: $\sum_{\tau\in H_1} f(t\, \mathrm{W}\, \tau) = 120$ (W stands for componentwise addition mod 2). Note that this check is not unique for $t^2 - 170t - 35$. For example we may replace H_1 by the subspace H_2 with basis {1000 1110), (0100 1101), (00101011), (0001 0001)}.

Let $G = H_1 \times \cdots \times H_n$. In some cases it is important to know whether there exists the check generated by the given subgroup H_j for the channel f: $G \to K$. For example (see Section 5), in the case where H_j is a cyclic group, the network implementation of the check can be essentially simplified.

For every $\omega \in \hat{G}$ $(G = H_1 \times \cdots \times H_n)$ we denote $\omega = (\omega_1, ..., \omega_n)$, $\omega \in \hat{G}$, $\omega_r \in \{0, 1, ..., |\,\hat{H}_r\,| - 1\}$, $r = 1, 2, ..., n$ (see Section 2). Then, for the given $f: G \to K$ there exists a check $(\delta_{H_j} \circledast f)(t) = \gamma\delta_{H_j}(t \odot \tau) + |\,H_j\,|/|\,G\,|$

$(\sum_{\xi \in G} f(\xi) - \gamma)$, (K) generated by the normal subgroup H_j iff for every $\omega = (\omega_1, \ldots, \omega_{j-1}, 0, \omega_{j+1}, \ldots, \omega_n)$,

$$\omega \in \Omega_f(\gamma, \tau). \tag{22}$$

Indeed, (22) follows from the proof of Theorem 1, in view of

$$\overline{\{\omega \mid \omega_j = 0\}}^{\perp} = H_j .$$

Example 5. Let channel $f_2 \colon G \to GF(11)$ (where $G = C_2 \times S_3$) is defined by Table I. The indexing of the elements $t \in G$ by vectors (t_1, t_2), $t_1 \in C_2$, $t_2 \in S_3$ is given in Table I. In this case $\omega = (\omega_1, \omega_2)$, $(\omega_1 \in C_2, \omega_2 \in S_3)$, $\omega_1 \in \{0, 1\}$, $\omega_2 \in \{0, 1, 2\}$. The indexing of the representation $\omega \in \hat{G}$ by vectors $\omega = (\omega_1, \omega_2)$ is given in Table III.

From this table it follows that $\bar{\Omega}_5 = \{(0, 0), (0, 1), (0, 2)\} = \Omega_{f_2}(2, 4)$. Hence by (22) C_2 is the subgroup of G, generating the cyclic check

$$f_2(t) + f_2(t \odot 6) = 2\delta_{C_2}(t \odot 4) + 1, \ (C_2 = \{0, 6\}), \ (GF(11)).$$

It follows from Tables II and III that if we consider f_2 as $f_2 \colon G \to C$, then a non-trivial cyclic check fro f_2 does not exist.

We consider now construction of linear checks for a device or a computer program calculating the system of functions $\{f^{(0)}, \ldots, f^{(s-1)}\}$, $f^{(j)} \colon G \to K$ $(j = 0, 1, \ldots, s-1)$. Let $G^{(l)}$ be come group with s elements. The system $\{f^{(0)}, \ldots, f^{(s-1)}\}$ may then be considered as a computation channel $f \colon G^{(l)} \times G \to K$ over the group $G^{(l)} \times G$, and the methods described in this section may be made of use in finding the checks for f (and consequently for the given system $\{f^{(0)}, \ldots, f^{(s-1)}\}$). In this connection we have an apparently quite difficult problem of optimal selection of a group $G^{(l)}$ of the given order $s = |G^{(l)}|$ minimizing the complexity of the check.

5. Implementation of Linear Checking Equations for the Computation Channel

We attribute an error e $(e \colon G \to K)$ to a channel $f \colon G \to K$ if the latter yields $f + e$, (K) instead of f. (In other words, we use the additive method to describe the influence of errors in the channel.)

The procedure of error detection or correction is divided in two steps, as is usually done in coding theory: first, we compute the results of the checks (1), called the error syndrome; secondly, we detect or correct errors by the computed syndrome. We give now the formal definitions.

Let K_j be some chosen fields and $f \colon G \to \bigcap_{j=1}^{m} K_j$ be the given channel with the system of checks $\delta_{H_j} \circledast f = \varphi_j + \lambda_j$, (K_j). Let $e \colon G \to \bigcap_{j=1}^{m} K_j$ be an error in the channel f. By the syndrome $S^{(e)}$ of an error e, we mean the system of functions $S_j^{(e)}\ G \rightarrow K_j$ defined as:

$$S_j^{(e)} \triangleq \delta_{H_j} \circledast (f + e) - \varphi_j - \lambda_j = \delta_{H_j} \circledast e, (K_j), (j = 1,..., m). \quad (23)$$

In this section we consider methods for syndrome computation. In practice, computation of the syndrome $S^{(e)}$ may be implemented with the aid of the computer program or the linear discrete network containing only the delay elements, the adder in the field K and elements realizing the group operation $\odot$. In the first case the quantity $\sum_{j=1}^{m} \| \delta_{H_j} \|$ (see preceding section) is the number of elementary addition in computing the syndrome $S^{(e)}$. In the second, it determines the complexity of the corresponding discrete network, i.e. the number of elements needed for its realization and the time for computing the syndrome (see Fig. 1, below).

Let $\{f^{(0)},..., f^{(s-1)}\}$ be the given system of functions $f^{(j)}$: $G \rightarrow K$, $(j = 0,...,$

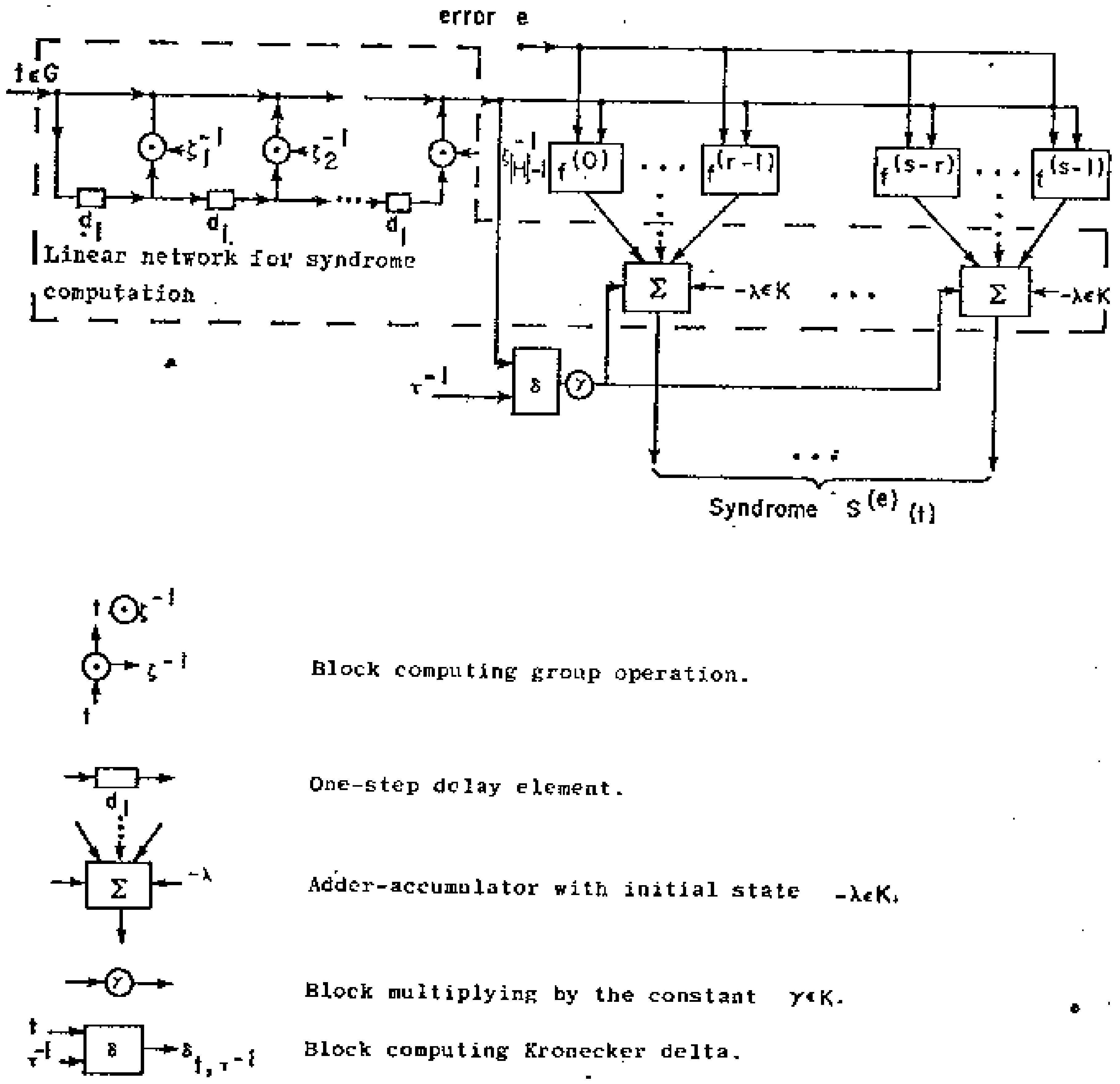

FIG. 1. Network implementation of one check for the system $\{f^{(0)},..., f^{(s-1)}\}$.

$s - 1$). We consider $\{f^{(j)}\}$ as a function $f: G^{(l)} \times G \to K$, where $G^{(l)} = \{0,..., s - 1\}$. The network implementation of one checking equation $\delta_H \circledast f = \varphi + \lambda, (K)$ is given in Fig. 1.

Here

$$\delta_H(j, \zeta) = \begin{cases} 1, & j \in H^{(l)} = \{0,..., r - 1\}, \zeta \in H = \{0, \zeta_1 ,..., \zeta_{|H|-1}\}; \\ 0, & \text{otherwise} \end{cases}$$

H being a normal subgroup of G and $H^{(l)}$ a normal subgroup of $G^{(l)}$; the jth right coset of $G^{(l)}$ with respect to $H^{(l)}$ is $\{jr, jr + 1,..., (j + 1)r - 1\}$, $(r = | H^{(l)}|$; $j = 0,..., s/r - 1)|$. As previously in Theorem 1, we suppose that $\varphi(t) = \gamma\delta_H(t \odot \tau), (K)$.

In the network of Fig. 1. signals corresponding to

$$f(t), f(t \odot \zeta_1^{-1}),..., f(f \odot \zeta_{|H|-1}^{-1}) \qquad \text{and} \qquad \delta_{\tau^{-1},t} , \delta_{\tau^{-1},t\odot\zeta_1^{-1}} ,..., \delta_{\tau^{-1},t\odot\zeta_{|H|-1}^{-1}}$$

are applied at successive instants of time to the input of the adders $\sum$ in the field K with initial state $-\lambda \in K$. For generation of $\varphi(t) = \gamma\delta_H(t \odot \tau)$, we make use of the fact that, by definition of δ_H , we have

$$\delta_H(t \odot \tau) = \delta_{\tau^{-1},t} + \sum_{j=1}^{|H|-1} \delta_{\tau^{-1},t\odot\zeta_j^{-1}} , (K).$$

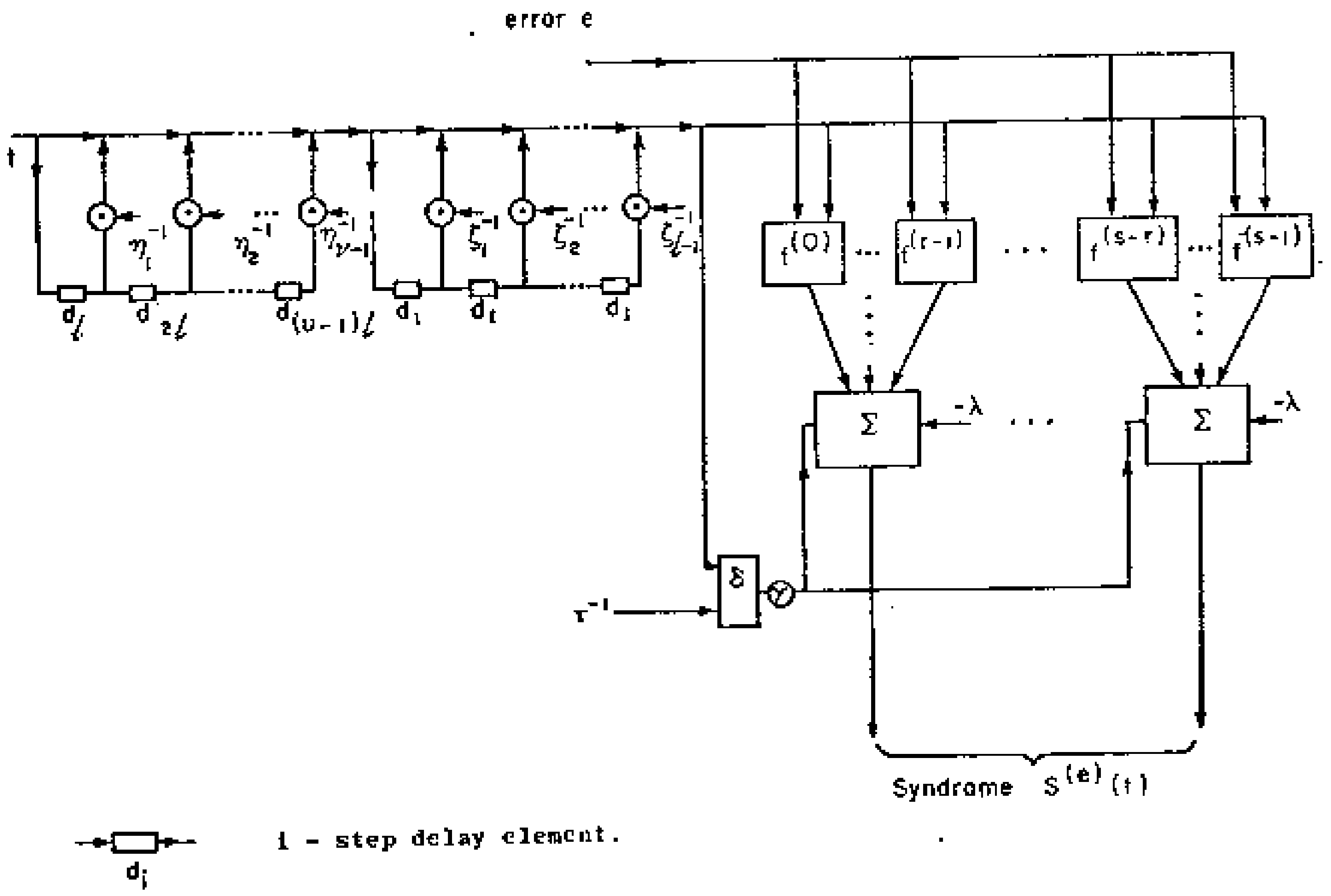

FIG. 2. Network implementation of a check for channel $f = \{f^{(0)},..., f^{(s-1)}\}$ in case H contains the subgroup $H' = \{0, \zeta_1 ,..., \zeta_{l-1}\}$.

Let H contain some subgroup $H' = \{0, \zeta_1, ..., \zeta_{l-1}\}$ (not necessarily normal in H), and let $|H|/l = \nu$ be the number of right cosets of H with respect to H', with representatives $0, \eta_1, ..., \eta_{\nu-1}$. The following block diagram (see Fig. 2) is then equivalent to that of Fig. 1.

To implement this network, we need only $(l + \nu - 2)$ delay elements and $(l + \nu - 2)$ elements realizing the group operation. Accordingly the network of Fig. 2. is preferable if H contains some non-trivial subgroup H'.

The network implementation of the given check $\delta_H \circledast f = \varphi + \lambda$, (K) can be further simplified if H is a cyclic subgroup of the original group G. The network implementation of a check $\delta_H \circledast f = \varphi + \lambda$, (K) ($\delta_H(\zeta) = 1$ iff $\zeta \in H$, H being a cyclic group with generator α) is given in Fig. 3.

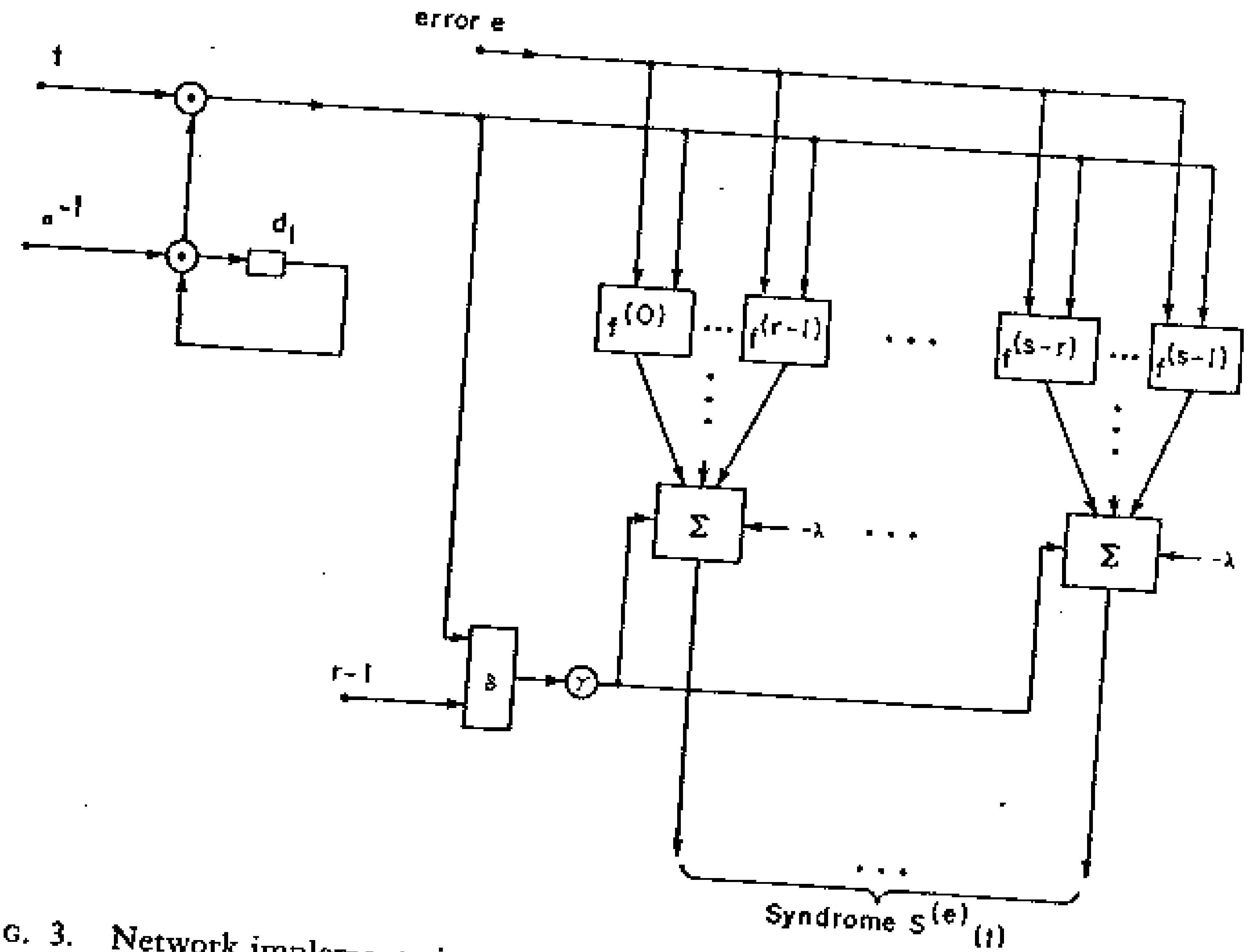

FIG. 3. Network implementation of channel $f = \{f^{(0)},...,f^{(s-1)}\}$ in case of the check, generated by the cyclic subgroup with generator α.

Here we have identity of H at the output of the delay element d_1 at the initial time and signals corresponding to α^{-1}, t, $\tau \in G$ are applied, at $|H|$ successive instants of time, to the inputs of the network. It should be noted that the complexity of the network of Fig. 3. does not depend on the cardinality $|H|$ of the chosen cyclic subgroup, which only affects the time required for the check.

Suppose now that the syndrome computation is implemented by a computer program.

Let $\delta_H \circledast f = \varphi + \lambda$, (K), $H = \{\zeta \mid \delta_H(\zeta) = 1\}$, H containing some non-trivial normal subgroups H_1, H_2 of group G, and let $\delta_{H_r}(\zeta) = 1$, iff $\zeta \in H_r$; $r = 1, 2$. If moreover,

$$\theta\delta_H = \delta_{H_1} \circledast \delta_{H_2}, \qquad \theta \in K, \tag{24}$$

$(\| \delta_{H_1} \| > 1, \| \delta_{H_2} \| > 1)$ then we need $\| \delta_{H_1} \| + \| \delta_{H_2} \| \leqslant \| \delta_H \|$ elementary additions to compute $S^{(e)}$. It is readily seen that (24) holds iff H is the smallest normal subgroup of G containing H_1 and H_2 and $\Theta = | H_1 \cap H_2 |$.

6. Error-Detecting and Correcting Capability of a System of Linear Checks for a Computation Channel

Let there be a system of m checks in some chosen fields K_j $(j = 1,..., m)$ constructed in accordance with Theorem 2 for the given channel $f: G \to \bigcap_{j=1}^m K_j$:

$$\delta_{H_j} \circledast f = \varphi_j + \lambda_j, (K_j), \qquad (j = 1,..., m). \tag{25}$$

Here $\delta_{H_j}(t) = 1$ iff $\tau \in H_j$, H_j being normal subgroups in G, $| H_j | > 1$, $\text{Im}\, \varphi_j \subseteq \bigcap_{j=1}^m K_j$ for all $j = 1,..., m$.

We shall consider two methods for detection or correction of an error e by the syndrome $S^{(e)}$ (see (23) in Section 5) namely memoryless and memory-aided decoding.

In memoryless decoding the value $e(t)$ is computed for the every $t \in G$ by $S^{(e)}(t)$; in memory-aided decoding $e = (e(0), e(1),..., e(| G | - 1))$ is computed by $S^{(e)} = (S^{(e)}(0), S^{(e)}(1),..., S^{(e)}(| G | - 1))$. (We suppose that elements of G are numbered by integers, $G = \{0,..., | G | - 1\}$). We note that the procedure of error detection and correction is simpler with memoryless decoding, but as will be shown in this section, the error-correcting capability of the given checking system (25) is reduced in this case.

We give the formal definitions. Let for any set E or errors, the error $e = 0$ belongs to E.

A set E of errors in a channel f with checks (25) is detected by memoryless decoding if, for any $e \in E$ and for every given $t \in G$, it follows from $e(t) \neq 0$ that there exists $j \in \{1,..., m\}$ such that $S_j^{(e)}(t) \neq 0$.

A set E of errors is corrected by memoryless decoding, if for any e_1, $e_2 \in E$ and for every given $t \in G$, it follows from $e_1(t) \neq e_2(t)$ that there exists $j \in \{1,..., m\}$ such that $S_j^{(e_1)}(t) \neq S_j^{(e_2)}(t)$.

A set E of errors in a channel f with checks (25) is detected by memory-aided decoding if, for any $e \in E$ it follows from $e \neq 0$ that there exist $j \in \{1,..., m\}$ and $t \in G$ such that $S_j^{(e)}(t) \neq 0$.

A set E of errors is corrected by memory-aided decoding if, for any $e_1, e_2 \in E$ it follows from $e_1 \neq e_2$ that there exist $j \in \{1, 2,..., m\}$ and $t \in G$ such that $S_j^{(e_1)}(t) \neq S_j^{(e_2)}(t)$.

Defining:

$$e_1(0) = 1;\ e_1(t_1) = \cdots = e_1(t_{[m/2]}) = -1;\ e_1(t) = 0 \text{ if } t \notin \{0, t_1, \ldots, t_{[m/2]}\},$$
$$e_2(t_{[m/2]+1}) = \cdots = e_2(t_m) = 1;\ e_2(t) = 0 \text{ if } t \notin \{t_{[m/2]+1}, \ldots, t_m\},$$

($t_j \in H_j$, $t_j \neq 0, j = 1,\ldots, m$), we have $\| e_1 \| = [m/2] + 1, \| e_2 \| = m - [m/2] \leqslant [m/2] + 1$, $e_1(0) \neq e_2(0)$ but

$$S_j^{(e_1)}(0) = S_j^{(e_2)}(0) = \begin{cases} 0, & j = 1,\ldots, \left[\dfrac{m}{2}\right]; \\ 1, & j = \left[\dfrac{m}{2}\right] + 1,\ldots, m; \end{cases}$$

and errors e_1, e_2 with multiplicity $[m/2] + 1$ are not corrected.

Note that for correction with memoryless decoding, use may be made of a method analogous to the majority logic approach in error-correcting codes (see, e.g., Massey, 1963). Let $m = 2l + 1$ and $\| e \| \leqslant l$. Then for any $t \in G$, there are at lease $l + 1$ components with the same value $e(t)$ in a vector $S^{(e)}(t) = (S_1^{(e)}(t),\ldots, S_m^{(e)}(t))$. We thus have a simple means of error correction for a syndrome vector $(S_1^{(e)}(t),\ldots, S_m^{(e)}(t))$.

We now consider the maximal multiplicites of errors detected or corrected with memory-aided decoding.

For a given system (25) or orthogonal checks, we denote $M(\sigma_1, \ldots, \sigma_m)$ as the set of all $t \in G$ such that there exist $t_j \in H_j$, $t_j \neq 0$, and

$$t = \sigma_1 t_1 \odot \sigma_2 t_2 \odot \cdots \odot \sigma_m t_m \triangleq \bigodot_{j=1}^{m}{}' \sigma_j t_j,\ \sigma_j \in \{0, 1\},\ \sigma_j t_j \triangleq \begin{cases} t_j, & \sigma_j = 1 \\ 0, & \sigma_j = 0 \end{cases};$$

$j = 1,\ldots, m$. We also resuire that for any $\sigma = (\sigma_1, \ldots, \sigma_m)$ and $\sigma' = (\sigma_1', \ldots, \sigma_m')$, $(\sigma \neq \sigma')$

$$M(\sigma) \cap M(\sigma') = \varnothing \ (\varnothing \text{ is the empty set}). \tag{27}$$

(Note that by setting

$$\sigma' = (\underbrace{0,\ldots, 0,}_{i} 1, 0,\ldots, 0), \qquad \sigma = (\underbrace{0,\ldots, 0,}_{j} 1, 0,\ldots, 0)$$

we have by (27), $H_i \cap H_j = \{0\}$, $(i \neq j)$.) If for a system (25) of checks the condition (27) holds, then the number m of checks satisfies

$$m \leqslant \log_2 |G|. \tag{28}$$

Condition (27) essentially implies that $H_1 \times \cdots \times H_m$ is isomorphic to a subgroup of G and this is a very strong restriction on the system (25) of checks.

THEOREM 4. *For any channel* $f: G \to \bigcap_{j=1}^{m} K_j$ *and any system of m checks* $\delta_{H_j} \circledast f = \varphi_j + \lambda_j$ $(j = 1,\ldots, m)$ *satisfying* (27), *we have for memory-aided decoding:*

(i) *All errors with multiplicity at most* $2^m - 1$ *are detected, and all those with multiplicity at most* $2^{m-1} - 1$ *are corrected.*

(ii) *There exist errors with multiplicity* 2^m *and* 2^{m-1}, *which are not detected and not corrected, respectively.*

Proof. (i) Let $e(t) \neq 0$ for some $t \in G$. We shall show that if the error e is not detected, then for any vector $\sigma = (\sigma_1,\ldots, \sigma_m)$ $(\sigma_j \in \{0, 1\})$ there exists at least one $t_\sigma \in t \bigcirc M(\sigma)(t \bigcirc M(\sigma) = \{\zeta \mid \zeta = t \bigcirc \nu, \nu \in M(\sigma)\})$ such that $e(t_\sigma) \neq 0$. Since from (27) $|\bigcup_\sigma M(\sigma)| \geqslant 2^m$, then it follows from the above that $\| e \| \geqslant 2^m$.

The proof will be by induction on $\| \sigma \| = \sum_{j=1}^{m} \sigma_j$.

Let $e(t) \neq 0$ and set $\sigma = (0,\ldots, 0)$. Then $\| \sigma \| = 0$, and setting $t_\sigma = t$ we have $t \in t \bigcirc M(\sigma)$ and $e(t_\sigma) \neq 0$.

Let it further be assumed that $e(t) \neq 0$, e is not detected and for any σ' such that $\| \sigma' \| = l$ $(l = 1,\ldots, m - 1)$ there exists $t_{\sigma'} \in t \bigcirc M(\sigma')$ such that $e(t_{\sigma'}) \neq 0$. Set $\| \sigma \| = l + 1$. By the definition of $M(\sigma)$, there exist σ' and some non-trivial subgroup H_i $(i \in \{1, 2,\ldots, m\})$ such that $\| \sigma' \| = l$ and

$$M(\sigma) = \bigcup_{\zeta \in H_i - \{0\}} M(\sigma') \bigcirc \zeta. \tag{29}$$

Since by the assumption $e(t_{\sigma'}) \neq 0$, and if e is not detected then

$$\sum_{\zeta \in H_i} e(t_{\sigma'} \bigcirc \zeta^{-1}) = e(t_{\sigma'}) + \sum_{\zeta \in H_i - \{0\}} e(t_{\sigma'} \bigcirc \zeta^{-1}) = 0, \ (K_i),$$

and there exists at least one $\zeta \in H_i - \{0\}$ such that if we set $t_\sigma = t_{\sigma'} \bigcirc \zeta^{-1}$ then $e(t_\sigma) \neq 0$. But $t_{\sigma'} \in t \bigcirc M(\sigma')$, and in view of (29) we have $t_\sigma = t_{\sigma'} \bigcirc \zeta^{-1} \in t \bigcirc M(\sigma)$. Consequently, all e such that $0 < \| e \| \leqslant 2^m - 1$ are detected.

Let now $\| e_1 \| \leqslant 2^{m-1} - 1$, $\| e_2 \| \leqslant 2^{m-1} - 1$, $e_1 \neq e_2$. Then $e \triangleq e_1 - e_2$, $e \neq 0$, $\| e \| < 2^m$, e is detected and there exists $t \in G$, $j \in \{1, 2,\ldots, m\}$ such that $S_j^{(e)}(t) = S_j^{(e_1)}(t) - S_j^{(e_2)}(t) \neq 0$. Consequently, all errors multiplicity at most $2^{m-1} - 1$ are corrected.

(ii) We now construct the non-detected error e_0 with multiplicity 2^m. Let us fix arbitrary $t_j \in H_j$ $(t_j \neq 0)$, $j = 1,\ldots, m$ and set

$$e_0(t) = \begin{cases} (-1)^{\|\sigma\|}, & \text{if there exists } \sigma = (\sigma_1,\ldots, \sigma_m) \text{ such that } t = \bigodot_{j=1}^{m} \sigma_j t_j; \\ 0, & \text{otherwise.} \end{cases} \tag{30}$$

It follows by (30) that $\| e_0 \| = 2^m$. We show now that for any $t \in G$ and $j \in \{1,..., m\}$, $S_j^{(e_0)}(t) = \sum_{\zeta \in H_j} e_0(t \odot \zeta^{-1}) = 0, (K_j)$.

If for some $t \in G$ and some $\zeta \in H_j$, $e_0(t \odot \zeta^{-1}) \neq 0$ then in view of (30) there can be found σ such that $t \odot \zeta_j^{-1} = \bigodot_{i=1}^{m} \sigma_i t_i$ and

$$S_j^{(e_0)}(t) = \sum_{\zeta \in H_j} e_0(t \odot \zeta^{-1}) = e_0\left(\bigodot_{i=1}^{m} \sigma_i t_i\right) + \sum_{\zeta \in H_j - \{0\}} e_0\left(\bigodot_{i=1}^{m} \sigma_i t_i \odot \zeta^{-1}\right)$$

$$= e_0\left(\bigodot_{i=1}^{m} \sigma_i t_i\right) + \sum_{\zeta \in H_j - \{0\}} e_0\left(\bigodot_{i=1}^{j} \sigma_i t_i \odot \zeta^{-1} \odot \bigodot_{i=j+1}^{m} \sigma_i t_i\right), (K_j) \qquad (31)$$

(Here we use the fact that H_j and $H_{j+1} \times \cdots \times H_m$ are normal subgroups of G with only the identity in common.) Now, if $\sigma_j = 0$, then in view of (30), (27),

$$e_0\left(\bigodot_{i=1}^{j} \sigma_i t_i \odot \zeta^{-1} \odot \bigodot_{i=j+1}^{m} \sigma_i t_i\right) \neq 0 \qquad \text{iff} \quad \zeta^{-1} = t_j$$

and by (30) we have

$$\sum_{\zeta \in H_j - \{0\}} e_0\left(\bigodot_{i=1}^{j} \sigma_i t_i \odot \zeta^{-1} \odot \bigodot_{i=j+1}^{m} \sigma_i t_i\right) = (-1)^{\|\sigma\|+1}, (K_j).$$

Hence, by (31), (30)

$$S_j^{(e_0)}(t) = (-1)^{\|\sigma\|} + (-1)^{\|\sigma\|+1} = 0, (K_j), (j = 1,..., m).$$

Analogically, if $\sigma_j = 1$ then in view of (30), (27) we see that

$$e_0\left(\bigodot_{i=1}^{j} \sigma_i t_i \odot \zeta^{-1} \odot \bigodot_{i=j+1}^{m} \sigma_i t_i\right) \neq 0 \qquad \text{iff} \quad \zeta^{-1} = t_j^{-1},$$

and

$$\sum_{\zeta \in H_j - \{0\}} e_0\left(\bigodot_{i=1}^{j} \sigma_i t_i \odot \zeta^{-1} \odot \bigodot_{i=j+1}^{m} \sigma_i t_i\right) = (-1)^{\|\sigma\|-1}, (K_j).$$

(Note that $\| \sigma \| > 1$ since $\sigma_j = 1$.) Consequently, by (31), (30)

$$S_j^{(e_0)}(t) = (-1)^{\|\sigma\|} + (-1)^{\|\sigma\|-1} = 0, (K_j), \qquad (j = 1,..., m)$$

and e_0 is not detected.

To conclude this proof, we note that existence of non-corrected errors with multiplicity 2^{m-1} follows from the fact that otherwise any error with multiplicity 2^m would be detected.

Thus, it follows from Theorems 3 and 4 that the error-detecting and correcting capabilities of a system of m orthogonal checks do not depend on field K and increase exponentially on transition from memoryless to memory-aided decoding.

EXAMPLE 6. For the pseudoboolean channel $f(t) = t^2 - 170t - 35$, $f: C_2^8 \to C$ from Example 4, Section 4 we have constructed two checks $\sum_{\tau \in H_i} f(t \mathrel{W} \tau) = 120$ $(i = 1, 2)$, H_1, H_2 have been described in Example 4. It is easy to verify that these checks are orthogonal and the condition (27) is satisfied. Thus from Theorems 3 and 4 these two checks detect all double errors and correct all single errors for memoryless decoding, detect all triple errors and correct all single errors for memory-aided decoding.

7. Orthogonal Checks for Computation Channels and Error-Correcting Codes

We consider in this section properties of error correcting codes generated by systems of orthogonal checks for computation channels.

We recall some basic definitions. Let $V_{g,K}$ be a linear space over the field K of dimension g, $d(\cdot;\cdot)$ being the Hamming metric in $V_{g,K}$, i.e. for any f_1, $f_2 \in V_{g,K}$, $d(f_1; f_2) = \| f_1 - f_2 \|$ — the number of non-zero components in the vector $f_1 - f_2$. A set $F \subseteq V_{g,K}$ is called the error-correcting code over K with distance $d(F)$, if $\min_{f_1, f_2} d(f_1; f_2) = d(F)$. It is called a linear (g, h)-code over K if it is an h-dimensional subspace of $V_{g,K}$, in which case it may also be defined by its $((g - h) \times g)$ check matrix (F_c) over K, i.e. $f \in F$ iff $(F_c)f = 0, (K)$. (32) The density of parity checks for the (g, h)-code F is defined as

$$\mu(F) = \frac{1}{(g - h)g} \sum_{i,j} \| (F_c)_{i,j} \|.$$

The coding and decoding procedures may be simplified on decreasing of $\mu(F)$, but this leads also to reduction of a transmission rate $R(F) = gh^{-1}$ of a code F (see, e.g., Gallager, 1963). We denote by $f(t)$ the tth component of the code vector $f \in F$ $(t = 0, 1, \ldots, g - 1)$.

A function $\sigma: \{0, 1, \ldots, g - 1\} \to \{0, 1, \ldots, g - 1\}$ is called an automorphism of a code F if for any $f \in F$ we have $f(\sigma) \in F$, where $(f(\sigma))(t) \triangleq f(\sigma(t))$, $t = 0, \ldots, g - 1$. The set of all automorphisms of F is a group Aut(F) which affects the complexity of the coding and decoding procedures (see, e.g., MAC WILLIAMS, 1964). If, for example, Aut(F) contains the group of cyclic translations of vectors from F, then we have an important class of cyclic codes. Analysis of Aut(F) and construction of codes with the given Aut(F) is an important and difficult problem in coding theory (MAC WILLIAMS, 1964).

We consider now the error correcting codes generated by systems of orthogonal checks for computation channels.

THEOREM 5. *For a given system of m checks in the field K satisfying* (27) *we denote*

$$F = \{f \mid \delta_{H_j} \circledast f = \varphi_j + \lambda_j, (K); H_j \text{ normal subgroups of } G\ (j = 1,..., m)\}. \qquad (33)$$

Then

(i) *for any $\varphi_j: G \to K$, $\lambda_j \in K$, F is an error correcting code over K with Hamming distance $d(F) = 2^m$;*

(ii) *for $\varphi_j = 0$, $\lambda_j = 0$, (K), $(j = 1,..., m)$, F is a linear $(|G|, |G| R(F))$-code with $d(F) = 2^m$, $R(F) = \prod_{i=1}^m (1 - |H_i|^{-1})$ and $G \subseteq \mathrm{Aut}(F)$.*

Proof. (i) For any $f_1, f_2 \in F$ we set $e = f_1 - f_2$, (K). Then $\delta_{H_j} \circledast e = 0$, (K), $(j = 1,..., m)$, e is not detected by memory-aided decoding and, by Theorem 4, $\| e \| \geqslant 2^m$ and $d(F) \geqslant 2^m$.

On the other hand there exists the error e_0 such that $\| e_0 \| = 2^m$ and e_0 is not detected by memory-aided decoding (see Theorem 4, (ii)). Hence, if $f \in F$ then $f + e_0 \in F$, (K), and $d(F) = 2^m$.

(ii) If $\varphi_j = 0$, $\lambda_j = 0$ $(j = 1,..., m)$, then F is linear space over K. By (27) $H_1 \times \cdots \times H_m$ is isomorphic to some normal subgroup of G and for any ordering elements of subgroups H_j we have $t = (t_1, ..., t_m, t_{m+1})$ where $t_j \in \{0,..., |H_j| - 1\}$ $(j = 1,..., m)$, $t_{m+1} \in \{0,..., |G| \prod_{j=1}^m |H_j|^{-1}\}$. Then $f \in F$ iff

$$\sum_{t_j=0}^{|H_j|-1} f(t_1, ..., t_{j-1}, t_j, t_{j+1}, ..., t_m, t_{m-1}) = 0 \qquad (j = 1,..., m)$$

for all $t_{m+1} \in \{0,..., |G| \prod_{j=1}^m |H_j|^{-1}\}$. Hence if $|G| = g$, $R(F) = gh^{-1}$ then

$$h = \dim F = |G| R(F) = \frac{|G|}{\prod_{j=1}^m |H_j|} \prod_{j=1}^m (|H_j| - 1) = |G| \prod_{j=1}^m (1 - |H_j|^{-1}).$$

For any $f \in F$ and $\tau \in G$ we set $f_\tau(t) = f(t \odot \tau)$ then $f_\tau \in F$ and $G \subseteq \mathrm{Aut}(F)$.

We note that for a code F generated by a system of orthogonal homogeneous checks with $\varphi_j = 0$, $\lambda_j = 0$ $(j = 1,..., m)$ if $f \in F$ then for any $\psi: G \to K$ $f \circledast \Psi \in F$, $\psi \circledast f \in F$ and F is a two side ideal in the group algebra of the group G over the field K. We note also that code F is a special case of the low density parity check codes considered by Gallager (1963) and one may construct by Theorem 5 linear codes F over the given field K with the fixed Hamming distance $d(F) = 2^m$, with transmission rate $R(F)$ asymptotically $(|G| \to \infty)$ equals to one and with the density of checks $\mu(F)$ asymptotically equals to zero. For example, we may set $G = \prod_{j=1}^m H_j$, $|H_1| = \cdots = |H_m| = |H|$, then by Theorem 5 we have a linear $(|H|^m, (|H| - 1)^m)$ code F over K with $d(F) = 2^m$ and if $|G| \to \infty$, then $|H| \to \infty$, $\lim_{|H| \to \infty} R(F) = \lim_{|H| \to \infty} (1 - |H|^{-1})^m = 1$ and for $m > 1$ $\lim_{|H| \to \infty} \mu(F) = \lim_{|H| \to \infty} |H|^{-(m-1)} = 0$.

RECEIVED: June 17, 1977; REVISED: July 24, 1978

References

Apple, G., and Wintz, P. (1970), Calculation of Fourier transform on finite Abelian groups, *IEEE Trans. Inform. Theory* **IT16**, 233–236.

Dornhoff, L. (1971), "Group Representation Theory," Dekker, New York.

Gallagher, R. G. (1963), "Low Density, Parity-Check Codes," MIT Press, Cambridge, Mass.

Karpovsky, M. G. (1977a), Error detection in digital devises and computer programs with the aid of recurrent equations over finite commutative groups, *IEEE Trans. Comput.* **C-26**, 208–218.

Karpovsky, M. G. (1977b), Harmonic analysis over finite commutative groups in linearization problems for systems of logical functions, *Inform. Contr.* **33**, 142–165.

Karpovsky, M. G. (1977c), Fast Fourier transforms on finite non-Abelian groups, *IEEE Trans. Comput.* **C-20**, October, 1028–1030.

Karpovsky, M. G. (1976), "Finite Orthogonal Series in the Design of Digital Devises," Wiley, New York.

Karpovsky, M. G., and Trachtenberg, E. A. (1977a), Some optimization problems for convolution systems over finite groups, *Inform. Contr.* **34**, 1–22.

Karpovsky, M. G., and Trachtenberg, E. A. (1977b), Linear checking equations and error correcting capability for computation channels, *in* "Proceedings IFIP Congress, 1977," North-Holland, Amsterdam.

MacWilliams, J. (1964), Permutation recoding of systematic codes, *Bell System Tech. J.*, January, 485–505.

Massey, J. L. (1963), "Threshold Decoding," MIT Press, Cambridge, Mass.

Opferman, D. C., and Tsao-Wo, N. T. (1971), On class of rearrangeable switching networks, *Bell Systems Tech. J.* **50**, 1579–1618.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium

Hence, using (34) and Lemma 2 with $\beta^{(\mathbf{C})} = 1 - \alpha^{(\mathbf{C})}$, we have

$$|G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)| > (1-\alpha^{(C)})|G^{(\mathbf{1})}(k_1,\ldots,k_s)|. \tag{39}$$

Summing over $\mathbf{C} \in \{0,1\}^s$ and using (33), we obtain

$$\sum_{\mathbf{C}\in\{0,1\}^s} |G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)| > (2^s-1)|G^{(\mathbf{1})}(k_1,\ldots,k_s)|. \tag{40}$$

We shall now show that

$$\bigcap_{\mathbf{C}\in\{0,1\}^s} G_M^{(\mathbf{1},C)}(k_1,\ldots,k_s) \neq \emptyset. \tag{41}$$

By (40)

$$|\bigcup_{\mathbf{C}} \overline{G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)}| \leq$$

$$\leq \sum_{\mathbf{C}} |\overline{G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s})| < |G^{(\mathbf{1})}(k_1,\ldots,k_s)|$$

(where the bar denotes the complementation: $\overline{G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)} = G^{(\mathbf{1})}(k_1,\ldots,k_s) - G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)$

and

$$|\bigcap_{\mathbf{C}} G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)| = |\overline{\bigcup_{\mathbf{C}} \overline{G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)}}| > 0$$

which implies (41).

Thus, there exists $\xi \in G(k_1,\dots,k_s)$ such that $\xi^{(\mathbf{1})} \in \bigcap_{\mathbf{C}\in\{0,1\}^s} G_M^{(\mathbf{1},\mathbf{C})}(k_1,\dots,k_s)$. It then follows from (35) that for this ξ, $\xi^{(\mathbf{C})} \subseteq M^{(\mathbf{C})}$ for all $\mathbf{C} \in \{0,1\}^s$, and so, in view of (22), (23), we have $\xi \subseteq M$, completing the proof of the theorem.

Note that, since $\mathbf{0} \in M$, we have $|M^{(\mathbf{0})}| = |G^{(\mathbf{0})}| = 1$, $\mu^{(\mathbf{0})}(M^{(\mathbf{0})}) = 1$; throughout the sequel, therefore, when using Theorem 3 we shall always assume, in accordance with (33), (34), that $\alpha^{(\mathbf{0})} = 0$.

Theorem 3 gives us sufficient conditions for the existence of a subgroup ξ with $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$ in $M \subseteq G$. To state corresponding conditions when, say, $k_j = 0$, we need only apply Theorem 3 to the group $\prod_{i\neq j} E(n_i)$.

4.3. We now turn to the question of linear codes in finite Abelian groups. Let $F \subseteq G$ be a set of errors and put

$$\ominus(F) = \{e \ominus f \,|\, e,f \in F\}$$

where $\ominus$ denotes componentwise subtraction of vectors $e = (e_1,\dots,e_s)$ and $f = (f_1,\dots,f_s)$ $(e_i, f_i \in E(n_i)$, subtraction of each f_i from e_i being performed mod $q_i (i=1,\dots,s))$.

<u>Theorem 4.</u> Let $R \subseteq G = \prod_{i=1}^{s} E(n_i)$, $F \subseteq G$ $(\mathbf{0} \in F \cap R)$, and suppose there exist $\alpha^{(\mathbf{C})} (\mathbf{C} = (C_1,\dots,C_s) \in \{0,1\}^s$, $\mathbf{C} \neq \mathbf{0}$; $0 < \alpha^{(\mathbf{C})} < 1)$

such that

$$\begin{cases} \sum\limits_{\mathbb{C}\neq\emptyset} \alpha^{(\mathbb{C})} = 1 \\ \prod\limits_{i=1}^{s} (q_i^{k_i}-1)^{c_i} < \alpha^{(\mathbb{C})}(\mu^{(\mathbb{C})}(\overline{R^{(\mathbb{C})}} \cup \theta^{(\mathbb{C})}(E)))^{-1} \end{cases} \tag{42}$$

for all $\mathbb{C} \neq \emptyset$. Then there exists a linear code ξ in G which corrects the error set F and satisfies the conditions $|\xi| = \prod\limits_{i=1}^{s} q_i^{k_i}$ and $\xi \subseteq R$.

Proof. A linear code ξ in G corrects a set F iff $\xi \cap \theta(F) = \{\emptyset\}$. Set $M = (R-\theta(F)) \cup \{\emptyset\}$. Then $\xi \subseteq R$ and ξ corrects the set F iff $\xi \subseteq M$. For any $\mathbb{C} \neq \emptyset$, we have $M^{(\mathbb{C})} = R^{(\mathbb{C})}-\theta^{(\mathbb{C})}(F)$ and

$$\begin{aligned} 1-\mu^{(\mathbb{C})}(M^{(\mathbb{C})}) &= (|G^{(\mathbb{C})}|-|R^{(\mathbb{C})}-\theta^{(\mathbb{C})}(F)|)\cdot|G^{(\mathbb{C})}|^{-1} = \\ &= |(G^{(\mathbb{C})}-R^{(\mathbb{C})})\cup\theta^{(\mathbb{C})}(F)|\cdot|G^{(\mathbb{C})}|^{-1} = \mu^{(\mathbb{C})}(\overline{R^{(\mathbb{C})}}\cup\theta^{(\mathbb{C})}(F)). \end{aligned} \tag{43}$$

Applying Theorem 3 and using (43), we obtain the sufficient conditions of Theorem 4.

When using Theorem 4 to look for the parameters $k_1,\ldots,k_s$ of a linear code $\xi \subseteq R$ correcting an error set E, we must check 2^s-1 conditions (42); this shows the advantage of using Theorem 4 when the number s of distinct primes in the direct-product decomposition of G is small.

The number of elements $|\xi|$ of a code ξ found with the aid of Theorem 4 depends on the choice of the parameters $\alpha^{(\mathbf{C})}$ for all $\mathbf{C} \in \{0,1\}^s$. This motivates the following corollary, which gives a sufficient condition that is more convenient, though coarser.

Corollary 3. A sufficient condition for the existence of a code $\xi \subseteq R$, where $R \subseteq G = \prod_{i=1}^{s} F(n_i)$, $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$ $(1 \leq k_i \leq n_i)$, correcting the error set F $(\mathbf{0} \in R \cap F)$, is that

$$\prod_{i=1}^{s} (q_i^{k_i}-1)^{C_i} < (\sqrt[s]{2}-1)^{\|\mathbf{C}\|}(\mu^{(\mathbf{C})}(\overline{R^{(\mathbf{C})}} \cup \theta^{(\mathbf{C})}(F)))^{-1} \qquad (44)$$

for all $\mathbf{C} = (C_1,\ldots,C_s) \in \{0,1\}^s$ $(\mathbf{C} \neq \mathbf{0})$, where $\|\mathbf{C}\| = \sum_{i=1}^{s} C_i$.

Proof. The corollary follows from Theorem 4 with $\alpha^{(\mathbf{C})} = (\sqrt[s]{2}-1)^{\|\mathbf{C}\|}$, in view of the fact that

$$\sum_{\mathbf{C} \neq \mathbf{0}} (\sqrt[s]{2}-1)^{\|\mathbf{C}\|} = \sum_{j=1}^{s} (\sqrt[s]{2}-1)^{j} \binom{s}{j} = 1.$$

4.4 We now consider the determination of a linear code ξ correcting a given error set and satisfying constraints of the type $\xi \subseteq R$.

<u>Theorem 5</u>. Let $R, F \subseteq G = \prod_{i=1}^{s} E(n_i)$, $\mathbf{0} \in R \cap F$. Let N_ξ be the number of linear codes ξ in G that correct the error set F and satisfy the conditions $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$ $(1 \leqslant k_i \leqslant n_i)$ and $\xi \subseteq R$.

Let $P(\xi) = N_\xi \cdot |G(k_1,\ldots,k_s)|^{-1}$.

If there exist $\alpha^{(\mathbf{C})}$ $(\mathbf{C}=(C_1,\ldots,C_s) \in \{0,1\}^s,\ \mathbf{C} \neq \mathbf{0},\ \alpha^{(\mathbf{C})}>0)$ and $0 \leqslant P_0 \leqslant 1$ such that

$$\begin{cases} \sum\limits_{\mathbf{C}\neq\mathbf{0}} \alpha^{(\mathbf{C})} = 1 - P_o & (45) \\ \prod\limits_{i=1}^{s} (q_i^{k_i}-1)^{C_i} > \alpha^{(\mathbf{C})}(\mu^{(\mathbf{C})}(\overline{R^{(\mathbf{C})}} \cup \theta^{(\mathbf{C})}(F)))^{-1} & (46) \end{cases}$$

then

$$P(\xi) > P_0 \qquad . \tag{47}$$

<u>Proof</u>. As before, define $G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)$ by (35) and let $M = (R-\theta(F))\cup\{\mathbf{0}\}$. In this situation, it follows from (43) that conditions (34) and (46) are equivalent; hence $|G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)|$ satisfies inequality (39). From (39) and (45) we have

$$\sum_{\mathbf{C}\neq\mathbf{0}} |G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)| > (2^s-1+P_0)|G^{(\mathbf{1})}(k_1,\ldots,k_s). \tag{48}$$

From (48) we obtain, proceeding as in the case of (40), (41)

$$|\cap G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)| > P_0|G^{(\mathbf{1})}(k_1,\ldots,k_s)|. \tag{49}$$

Next, it follows from (49) in view of (22), (23), (35) that if

$$\xi^{(\mathbf{1})} \in \bigcap_{\mathbf{C}\neq\mathbf{0}} G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)$$

then $\xi \subseteq M$. Hence, for $M = (R-\theta(F) \cup \{\mathbf{0}\}$, we obtain

$$N_\xi = |\bigcap_{\mathbf{C}\neq\mathbf{0}} G_M^{(\mathbf{1},\mathbf{C})}(k_1,\ldots,k_s)|.$$

Since for $k_i \neq 0$ $(i=1,\ldots,s)$ $|G^{(\mathbf{1})}(k_1,\ldots,k_s)| = |G\ (k_1,\ldots,k_s)|$ inequality (49) finally implies (47).

<u>Corollary 4</u>. A sufficient condition for a code ξ in the group $G = \prod_{i=1}^{s} E(n_i)$ correcting an error set F $(|\xi| = \prod_{i=1}^{s} q_i^{k_i}$, $\xi \subseteq R$, $\mathbf{0} \in R \cap F)$ to satisfy the inequality $P(\xi) > P_o$ is that

$$\prod_{i=1}^{s} (q_i^{k_i}-1)^{C_i} < (\sqrt[s]{2-P_o}-1.^{\|\mathbf{C}\|}(\mu^{(\mathbf{C})}(\overline{R^{(\mathbf{C})}} \cup \theta^{(\mathbf{C})}(F)))^{-1} \qquad (50)$$

for all $\mathbf{C} = (C_1,\ldots,C_s) \in \{0,1\}^s$ $(\mathbf{C}\neq\mathbf{0})$.

The proof of Corollary 4 follows from Theorem 5 with $\alpha^{(\mathbf{C})} = (\sqrt[s]{2-P_o}-1)^{\|\mathbf{C}\|}$ and the identity $\sum_{\mathbf{C}\neq\mathbf{0}} (\sqrt[s]{2-P_o}-1)^{\|\mathbf{C}\|} = 1-P_o$.

Comparing Theorem 4 and Theorem 5, and also Corollaries 3 and 4, one sees that (as in the case of codes in linear spaces) a relatively small reduction in the numbers $k_i (=1,\ldots,s)$ of information digits (in such a way that the transmission rate

$\sum_{i=1}^{s} k_i / \sum_{i=1}^{s} n_i$ does not change as $n_i \to \infty$) will bring the probability $P(\xi)$ close to unity, where $P(\xi)$ is the probability that any subgroup from $G(k_1,\dots,k_s)$ is the desired code ξ. This implies a very simple procedure for searching for linear codes in subsets of finite Abelian groups, yielding codes which are sufficiently close to optimal.

ups

that a necessary
code in a sub-
be sufficiently
ion fails to
that the code
aces by the weaker

l assume that each
f $\{0,\dots,q_1-1\}$,
on.
} (51)

denote the
dices lie in

5. Partially Linear Codes in Subsets of Abelian Gro

5.1. It follows from Theorem 4 and Corollary 3
condition for the existence of a nontrivial linear
set $R \subseteq G$ is that the measure $\mu^{(\Phi)}(R^{(\Phi)})$ should
close to unity for all $\Phi \in \{0,1\}^s$. If this condit
hold, we have no choice but to relinquish the deman
be linear, replacing it as in the case of linear sp
condition of partial linearity.

If $x \in G = \prod_{i=1}^{s} E(n_i)$ then, as before, we shal
of the first n_1 components of x is an element o
each of the next n_2 is in $\{0,\dots,q_2-1\}$, and so

Let $I_1 \subseteq \{1,\dots,n_1\}$, $I_i \subset \{\sum_{j=1}^{i-1} n_j+1,\dots,\sum_{j=1}^{i} n_j$

$(i=2,\dots,s)$, and let $P^{(I_1,\dots,I_s)}(M)$ (where $M \subseteq G$
projection of M onto the coordinate axes whose in
$\bigcup_{i=1}^{s} I_i$.

Definition 3. A code ξ in $G = \prod_{i=1}^{s} E(n_i)$ is said to be $(m_1,\ldots,m_s)$-linear $(m_i \leqslant n_i;\ i=1,\ldots,s)$ iff there exist I_i satisfying (51) such that $|I_i| = m_i$ $(i=1,\ldots,s)$ and $P^{(I_1,\ldots,I_s)}(\xi)$ is a linear code in G.

In order to find an $(m_1,\ldots,m_s)$-linear code ξ satisfying the constraint $\xi \subseteq R$, where R is a prescribed subset of G, we first find $I_1,\ldots,I_s$ such that $|I_i| = m_i$ $(i=1,\ldots,s)$ and $P^{(I_1,\ldots,I_s)}(R)$ is a subgroup of G, of order $\prod_{i=1}^{s} q_i^{m_i}$; we then try to find a code in this subgroup possessing the desired correcting capability.

Let ρ be a metric in the above group G, such that for $x = (x_1,\ldots,x_s) \in G$, $y = (y_1,\ldots,y_s) \in G$ $(x_i, y_i \in E(n_i),\ i=1,\ldots,s)$, the distance between x and y is

$$\rho(x,y) = \sum_{i=1}^{s} \rho_i(x_i,y_i)$$

where each ρ_i is a metric in the linear space $E(n_i)$ (e.g., the Hamming or Lee metric). We say that a code $\xi \subseteq G$ has distance d iff $\min_{x\ y;\ x,y\in\xi} \rho(x,y) = d$.

Theorem 6. Let $R \subset \prod_{i=1}^{s} E(n_i)$ and suppose that for some $m_1,\ldots,m_s$ $(1 \leqslant m_i \leqslant n_i,\ i=1,\ldots,s)$

$$|R| > \prod_{i=1}^{s} q_i^{n_i} - \prod_{i=1}^{s} \sum_{j=0}^{n_i-m_i} (q_i-1)^j \binom{n_i}{j}. \qquad (52)$$

Then there exists an $(m_1,\dots,m_s)$-linear code $\xi \subseteq R$ with distance d in the metric ρ, such that

$$|\xi| = \prod_{i=1}^{s} B_{q_i}^{\rho_i}(m_i,d). \tag{53}$$

(As before, $B_{q_i}^{\rho_i}(m_i,d)$ denotes the number of elements in a maximal linear code with distance d in the metric ρ_i, in the space $E(n_i)$ over $GF(q_i)$.)

Proof. It was shown in [7] that if condition (1) holds there exist

$$I_1 \subseteq \{1,\dots,n_1\},\dots,I_i \subseteq \{\sum_{j=1}^{i-1} n_j+1,\dots,\sum_{j=1}^{i} n_j\}$$

such that $|I_1| = m_1,\dots,|I_i| = m_i$ $(i=2,\dots,s)$ and

$P^{(I_1,\dots,I_s)}(R) = \prod_{i=1}^{s} E(n_i)$. Let ξ_i be a maximal linear code with distance d in the metric ρ_i in the space $E(n_i)$; we have $|\xi_i| = B_{q_i}^{\rho_i}(m_i,d)$. Then $\prod_{i=1}^{s}\xi_i$ is a code with distance d, which may be extended (by adding $\sum_{i=1}^{s}(n_i-m_i)$ coordinates to each vector of the code) to an $(m_1,\dots,m_s)$-linear code $\xi \subset R$ satisfying condition (53).

5.2. We are now interested in the asymptotic behavior $(n_i\to\infty,\ i=1,\dots,s)$ of the data-transmission rate of a maximal $(m_1,\dots,m_s)$-linear code in the group $G = \prod_{i=1}^{s} E(n_i)$, with distance

d in the Hamming or Lee metric ρ. That is to say, for $x = (x_1,\ldots,x_s) \in G$ and $y = (y_1,\ldots,y_s) \in G$ we have

$\rho(x,y) = \sum_{i=1}^{s} \rho_i(x_i,y_i)$ where ρ_i is the Hamming or Lee metric for all $i \in \{1,\ldots,s\}$.

The transmission rate $v(\xi)$ of a code $\xi \in G$ with $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$, is defined as

$$v(\xi) = (\sum_{i=1}^{s} k_i)\cdot(\sum_{i=1}^{s} n_i)^{-1}.$$

Let $v^{\rho}_{q_1,\ldots,q_s}(n_1,\ldots,n_s;\,|R|,d)$ be the transmission rate of a maximal $(m_1,\ldots,m_s)$-linear code in $R \subseteq G$ with distance d in the Hamming or Lee metric ρ.

<u>Corollary 5</u>. If $n_i \to \infty$, q_i are fixed $(i=1,\ldots,s)$, d is fixed, and $0 < \varepsilon_0 \leq |R| \prod_{i=1}^{s} q_i^{-n_i} < \varepsilon_1 < 1$, where ε_0 and ε_1 are constants, then

$$v^{\rho}_{q_1,\ldots,q_s}(n_1,\ldots,n_s;\,|R|,d) \gtrsim (\sum_{i=1}^{s} n_i q_i^{-1})(\sum_{i=1}^{s} n_i)^{-1} \quad (54)$$

(where $a \gtrsim b$ means that $\underline{\lim}_{n\to\infty} (a/b) \geq 1$).

<u>Proof</u>. Let $\hat{m}_1,\ldots,\hat{m}_s$ satisfy (52) for the given $|R|$, q_i,n_i $(i=1,\ldots,s)$, and assume moreover that if $m_i \geq \hat{m}_i$ $(i=1,\ldots,s)$ and $(m_1,\ldots,m_s) \neq (\hat{m}_1,\ldots,\hat{m}_s)$, then $m_1,\ldots,m_s$ do not satisfy (52) for the same $|R|$, q_i,n_i $(i=1,\ldots,s)$. Then, by (52),

$$\prod_{i=1}^{s} \sum_{j=0}^{n_i-\hat{m}_i} (1-q_i^{-1})^j \, q_i^{n_i-j} \binom{n_i}{j} \sim 1-|R| \prod_{i=1}^{s} q_i^{-n_i}$$

and

$$0.5 + \phi_o \, ((n_i-\hat{m}_i+0.5-n_i(1-q_i^{-1}))\cdot(n_i q_i^{-1}(1-q_i^{-1}))^{-\frac{1}{2}} \lesssim \qquad (55)$$

$$\lesssim \sum_{j=o}^{n_i-\hat{m}_i} (1-q_i^{-1})^j \, q_i^{n_i-j} \binom{n_i}{j} \lesssim 1-|R| \prod_{i=1}^{s} q_i^{-n_i}$$

(where $\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\tau^2/2} d\tau$).

Now if $0 < \varepsilon_0 \leq |R| \prod_{i=1}^{s} q_i^{-n_i} \leq \varepsilon_1 < 1$, then it follows from (55) that

$$n_i q_i^{-1} \lesssim \hat{m}_i \qquad (i=1,\ldots,s). \qquad (56)$$

By the definition of $v^{\rho}_{q_1,\ldots,q_s}(n_1,\ldots,n_s;\ |R|,d)$, it follows from Theorem 6 that

$$v^{\rho}_{q_1,\ldots,q_s}(n_1,\ldots,n_s;\ |R|,d) \geq (\sum_{i=1}^{s} \log_{q_i} B^{\rho_i}_{q_i}(\hat{m}_i,d))(\sum_{i=1}^{s} n_i)^{-1}. \qquad (57)$$

We know [1] that when ρ_i is the Hamming or Lee metric, then for any fixed d, $\log_{q_i} B^{\rho_i}_{q_i}(\hat{m}_i,d) \sim \hat{m}_i$ as $\hat{m}_i \to \infty$; thus (54) follows from (56) and (57), completing the proof.

Note that if $n_i \sim n_j$ $(i,j=1,\ldots,s)$, then from (54)

$$v^{\rho}_{q_1,\ldots,q_s}(n_1,\ldots,n_s;\ |R|,d) \gtrsim s^{-1} \sum_{i=1}^{s} q_i^{-1}. \qquad (58)$$

As a concluding remark, we note that (54) and (58) imply that, if n_i $(i=1,\dots,s)$ are sufficiently large, there exist non-trivial $(m_1,\dots,m_s)$-linear codes in arbitrary subsets of small measure.

Bibliography

1. Peterson, W. W., Error Correcting Codes, 2nd edition, MIT Press, Cambridge, Mass., 1972.

2. Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill, 1968.

3. Tenengolts, G. M., "Coding Systems with the Combined use of Pulse Tests" in: "Abstract and Structure Theory of Relay Systems" (in Russian), Izd. Nauka, Moscow (1966).

4. Lindström, B., "On Group and Nongroup Perfect.Codes in q Symbols", Math, Scand. 25, pp. 149-158, 1969.

5. Herzog, M., and Shönheim I., "Linear and Nonlinear Single-Error-Correcting Perfect Mixed Codes", Information and Control, vol. 18, N4, May, 1971.

6. Karpovsky, M. G., Milman, V. D., "On Subspaces Contained in Subsets of Finite-Dimensional Spaces Over a Finite Field" (to appear).

7. Karpovsky, M. G., Milman, V. D., "Coordinate Density of Sets of Vectors" (to appear).

Index terms:

Codes in subsets of linear spaces, codes in subsets of finite Abelian groups, partially linear codes in subsets of spaces and of groups, data-transmission rate of codes in subsets of spaces and of groups.

List of Special notations.

G	finite Abelian group;
$E(n)$	n-dimensional linear space over finite field;
ρ	metric in G or $E(n)$;
F	set of errors;
ξ	error correcting code in subsets of G or $E(n)$;
$\nu(\xi)$	transmission rate of the code ξ;
$G(k)$	set of all k-dimensional subspaces of n-dimensional space $E(n)$;
$G(k_1,\dots,k_s)$	set of all subgroups of order $\prod_{i=1}^{s} q_i^{k_i}$ in the group $G = \prod_{i=1}^{s} E(n_i)$, where $E(n_i)$-n_i-dimensional space over $GF(q_i)$;
$B_n^{\rho}(n,d)$	maximum number of elements in linear code $\xi \subseteq E(n)$ with distance d in the metric ρ.