LINEAR CHECKING EQUATIONS AND ERROR-CORRECTING CAPABILITY FOR COMPUTATION CHANNELS

M. G. KARPOVSKY
Tel-Aviv University
Tel-Aviv, Israel

E. A. TRACHTENBERG
Technion-Israel Institute of Technology
Haifa, Israel

Detection and correction of errors of arbitrary multiplicity which may appear in the input of computation channel (defined over an arbitrary finite group) or within the channel itself are investigated. The problem of building optimal checks for the given computation channel is solved and optimal checks are given for some important standard computer blocks (or standard subroutines).

Theorems are given for the solution of the problem of error detecting and correcting capability for a linear checks system by memoryless and memory-aided decoding procedures. This capability is group structure independent and grows exponentially when a transition from memoryless to memory-aided decoding is made.

1. ERROR DETECTION AND CORRECTION IN COMPUTATION CHANNELS

Let G be a finite group. By a computation channel f over G we mean any digital device or computer program computing the function $f : G \rightarrow C$, where C is the field of complex numbers. Examples of such channels over Abelian groups are the blocks of the arithmetic unit of a computer, networks whose operation is described by two - or many - valued switching functions, etc. As examples of channels over non-Abelian groups we note rearrangeable switching networks, [1] programs for interconnecting telephone lines, [2] linear control systems over non-Abelian groups, [3] etc.

By an error in a channel f we mean a catastrophic structural failure in a device or an error in a text of a program computing $f : G \rightarrow C$.

For error detection or correction in a channel f we use systems of linear checks

$$(a_i \circledast f)(t)=\sum_{\zeta\in G} a_i(\zeta)f(t\odot\zeta^{-1})=\varphi_i(t)+Q_i,$$

$$(i=1,2,\dots,k) . \qquad (1)$$

where $\circledast$ denotes the group convolution in G and $\odot$ the group operation in G ; $\zeta^{-1}\in G$ the inverse of ζ; $a_i,\varphi_i: G\rightarrow C$ are some "simple" checking functions and $Q_i\in C$ $(i=1,2,\dots,k)$.

To simplify the error detection and correction procedure, we confine our discussion to the case $a_i(\zeta)\in\{0,1\}$ for all $\zeta\in G$ and $i=1,2,\dots,k$. A network interpretation of one check of this type is illustrated in fig. 1. Here

$a(\zeta)=1$ <u>iff</u> $\zeta\in\{I,\zeta_1,\dots,\zeta_L\}$

(I is the identity of G).

In the network of fig. 1, signals corresponding to $f(t),f(t\odot\zeta_1^{-1}),\dots,f(t\odot\zeta_L^{-1})$ are applied at successive instants of time to the input of the adder Σ with initial state -Q. After L elementary additions and subtraction of φ(t), we obtain a result ("syndrome") of the check.

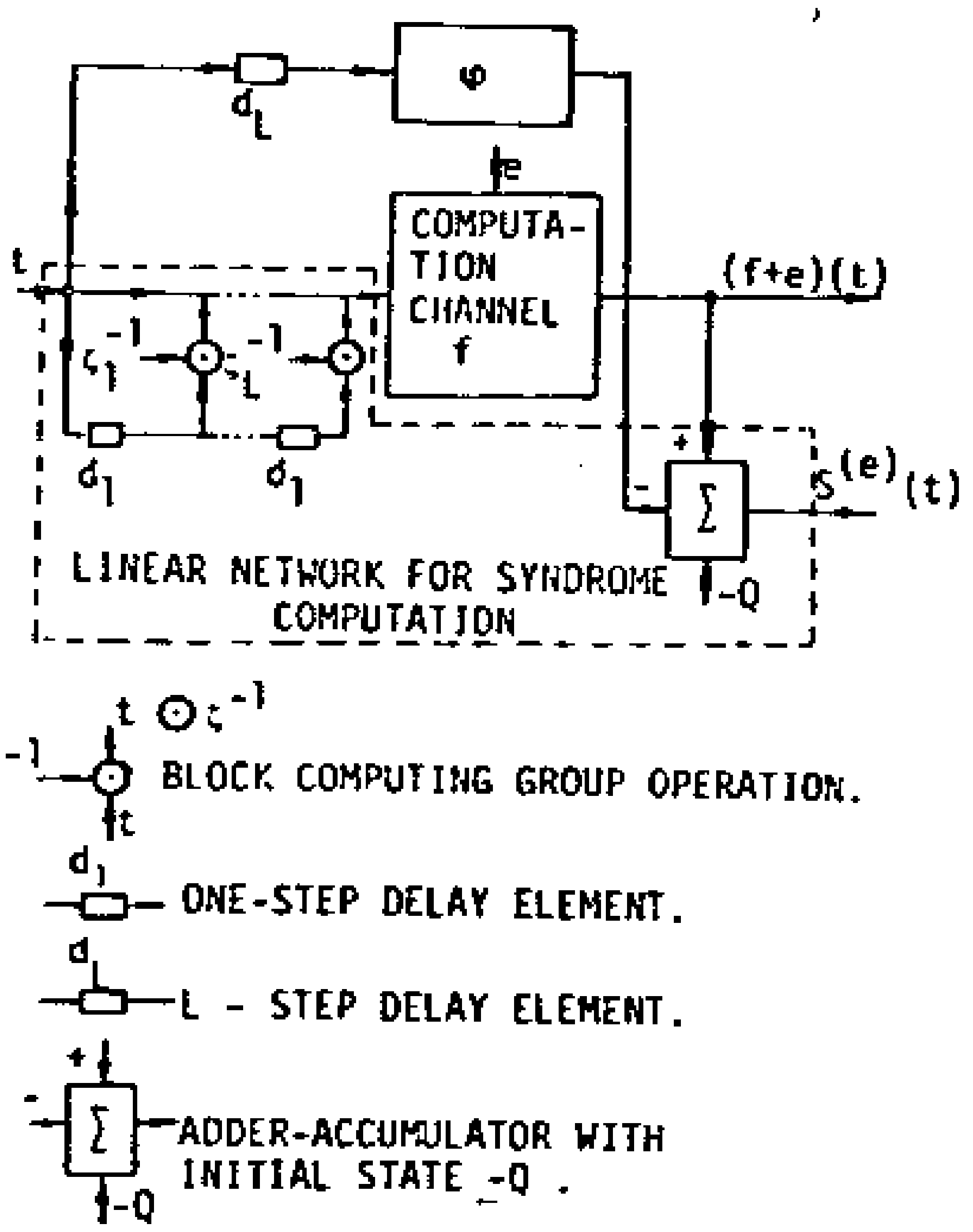

FIG. 1

Error detection with the aid of one check of the type (1) in channels over Abelian groups was considered in [4]. This work is devoted to the general case of error detection or correction in channels over arbitrary finite groups with the aid of systems of linear checks.

We attribute an error $e(e: G\rightarrow C)$ to a channel f , if the latter yields f + e instead of f .

<u>Definition 1.</u>

A syndrome $S^{(e)}=(S_1^{(e)},\dots,S_k^{(e)})$ of an error e for a channel f with checks

(1) is defined as follows:

$$S_i^{(e)}=(a_i \odot (f+e))-\varphi_i-Q_i=a_i \odot e,$$

$$(i=1,2,\dots,k) \ . \qquad (2)$$

Computation of the syndrome $S^{(e)}$ may be implemented with the aid of the computer program or the special linear network containing only the delay elements, the adder and elements realizing the group operation $\odot$ (see fig. 1).

We shall consider two methods for detection or correction of e by its syndrome $S^{(e)}$, namely memoryless decoding and memory-aided decoding.

Definition 2.

(i) A set E of errors in a channel f with checks (1) is detected by memoryless decoding if, for any $e\in E$, it follows from $e(t) \neq 0$ that there exists $i\in\{1,\dots,k\}$ such that $S_i^{(e)}(t)\neq 0$. (ii) A set E of errors is corrected by memoryless decoding if for any $e_1,e_2\in E$, it follows from $e_1(t)\neq e_2(t)$ that there exists $i\in\{1,\dots,k\}$ such that $S_i^{(e_1)}(t)\neq S_i^{(e_2)}(t)$.

Definition 3.

(i) A set E of errors is detected by memory-aided decoding if $S^{(e)}\neq 0$ for any $e\in E(e\neq 0)$. (ii) A set E of errors is corrected by memory-aided decoding if $S^{(e_1)}\neq S^{(e_2)}$ for any $e_1,e_2\in E(e_1\neq e_2)$.

We resort to methods of abstract harmonic analysis on G, which yield exact and convenient results from the computational viewpoint, for construction of the linear checks, and for evaluation of their error-detecting and correcting capability. Algorithms of fast Fourier transforms over G[5,6] are extremely useful in the implementation of these methods by computer programs. An analogous approach based on harmonic analysis over G was used, for functions on finite groups, in [3,7,8,9,10].

2. LINEAR CHECKING EQUATIONS FOR COMPUTATION CHANNELS

In this section we consider the problem of finding, for a given channel f, optimal functions $a: G \to \{0,1\}$, $(a\neq 0)$ $\varphi: G \to C$ and constant $Q \in C$ such that $a \odot f = \varphi + Q$. It is natural to use $\|a\|$, the number of nonzero values of the function a (or the Hamming weight of a) as the complexity criterion for the function a. The same criterion will be used for estimating the complexity of the function φ. (Note that the Hamming weight as a complexity criterion for functions defined on finite groups, figured also, for example in synthesis problems ~~of~~ optimal linear control systems for a given input/output pair [3].)

The problem thus consists in finding a_{opt} and φ_{opt} such that

$$\min_{a\odot f=\varphi+Q}(\|a\|+\|\varphi\|)=\|a_{opt}\|+\|\varphi_{opt}\| \ . \qquad ($$

We impose a further natural constrain on the class of checking functions a namely, $a(\zeta) = 1$ *iff* $\zeta\in G_j$ where (is any normal subgroup of G.

Fourier and inverse Fourier transforms may be defined for the function $f : G \to C$, as follows:

$$f(\omega) = d_\omega |G|^{-1} \sum_{t\in G} f(t)\, R_\omega(t^{-1}) \ , \qquad (4$$

$$f(t) = \sum_{R_\omega\in\hat{G}} \mathrm{trace}(\hat{f}(\omega)R_\omega(t)). \qquad (5$$

Here $|G|$ is the cardinality of G; $R_\omega(t)$ is the ω-th irreducible unitar representation of G in a space of di mension d_ω over the field C [11]; for any $t\in G$, $R_\omega(t)$ is a $(d_\omega \times d_\omega)$ unitary representations of G. (Construction methods for all non-equivalent irreducible unitary representations are to be found, for example, in [11]. In (5) $\hat{G}$ is the set of all non-eq valent irreducible representations of G For the Fourier transform $f\to\hat{f}$ on th group G defined by (4), (5) the usual properties of linearity, translation, convolution, Plancherel, Poisson, Wiene Khinchine theorems, etc. are valid (see e.g., [3]).

A subset $P\subseteq \hat{G}$ is said to be closed (notation $P=[P]$) if for any $R_\omega \notin P$ $(R_\omega\in\hat{G})$ we have $\mathrm{kern}\, R_\omega \subset \mathrm{kern}\, P$, where

$$\mathrm{kern}P= \bigcap_{R_\omega\in P} \mathrm{kern}R_\omega = \bigcap_{R_\omega\in P} \{t \mid R_\omega(t)=E\}$$

and E is an identity matrix.

We next denote

$$\sum_{R_\omega\in[P]} d_\omega^2 = \alpha([P]) \ , \qquad (6)$$

(for any $[P]\subseteq\hat{G}$ $\quad \alpha([P])\cdot|\mathrm{kern}[P]|=|G|$)

and for a given $f:G \to C$ and any $\gamma\in C, \tau\in G$

$$\Omega_f(\gamma,\tau)=\{R_\omega \mid \hat{f}(\omega)=d_\omega\gamma|G|^{-1}R_\omega(\tau)\}\cup\{R_o\}$$

$$(R_o(t) = 1 \text{ for any } t\in G \ ). \qquad (7)$$

Theorem 1.

Let for a given f, $[P] \subseteq \Omega_f(\gamma,\tau)$ for some $\gamma\in C$, $\tau\in G$. Then

$$\|a_{opt}\|+\|\varphi_{opt}\|\leq(1+|\mathrm{sign}\gamma|)|\mathrm{kern}[P]| \qquad (8)$$

$$\left(|\mathrm{sign}\gamma|=\begin{cases}1, & \gamma\neq 0;\\ 0, & \gamma=0.\end{cases}\right)$$

For the proof of Theorem 1 it suffices to put

$$a(t)=\begin{cases}1, & t\in \mathrm{kern}\ [P];\\ 0, & t\notin \mathrm{kern}\ [P].\end{cases}, \ \varphi(t)=\gamma a(t\odot\tau); \qquad (9)$$

and

$$Q=|\mathrm{kern}\,[P]|\ |G|^{-1}\Big(\sum_{\zeta\in G} f(\zeta)-\gamma\Big). \qquad (10)$$

We note also that if G_i is the given normal subgroup of G and $f:G\to C$ the given channel then the check $a^{\odot}f=\varphi+Q$

$$\text{with } a(t) = \begin{cases}1, & t\in G_i\\ 0, & t\notin G_i\end{cases}$$

and $\varphi(t)=\gamma a(t\odot\tau)$ exists iff $[\mathrm{kern} G_i] = \{R_\omega | R_\omega(t)=E \text{ for all } t\in G_i\} \subseteq \Omega(\gamma,\tau)$.

For the network implementation of $\varphi(t)=\gamma\, a(t\odot\tau)$ we can make use of the fact that from (9)

$$a(t\odot\tau)=a(\tau\odot t) = \sum_{\xi\in \mathrm{kern}[P]} \delta_{\tau^{-1},t\odot\xi}$$

(δ-denoting the Kronecker delta).

For the important case of groups of binary n-vectors with componentwise addition mod 2 we have $|G|=2^n$, $d_\omega=1$ for all $R_\omega\in\hat{G}$, R_ω is the ω-th Walsh function [8], $R_\omega(t)\in\{\pm1\}$ for all $R_\omega\in\hat{G}$ and $t\in G$; $\hat{G}$ is a multiplicative group isomorphic to G; $P=[P]$ iff P is a subgroup of $\hat{G}$, $\alpha([P])=|[P]|\in\{2^0,2^1,\dots,2^n\}$ and we can use the function $\Omega_f(\gamma)=\{R_\omega|\hat{f}(\omega)=2^{-n}\gamma\}\cup\{R_0\}$ instead of $\Omega_f(\gamma,\tau)$ in Theorem 1.

Of special interest is the particular case $a^{\odot}f=Q$ with $\varphi=0$. Although the relavant class of channels is relatively small, it will be seen below that a large variety of standard computer blocks (or standard subroutines) have fairly simple optimal checks of this type. Some important examples of chanels f, checks $a^{\odot}f=Q$ and the complexities $\|a\|$ of these checks are given in table 1.

Computation channel checks are given in the lower part of table 1 (nos. 7-10), for G a group of p-ary n-vectors with $\oplus$-componentwise addition mod p. In table 1, $X=(x_0,\dots,x_{n-1})$ denotes both the element $X\in G$ and the natural number $0\le X\le p^n-1$ i.e. $X=\sum_{i=0}^{n-1} x_i p^{n-1-i}$.

The upper part of table 1 (nos. 1-6) is devoted to the special case p=2.

In table 1, $\mathbb{1}=(1,\dots,1)$, $\mathbb{0}=(0,\dots,0)$, $\mathbb{P}-\mathbb{1}=(p-1,\dots,p-1)$, $J=(j,\dots,j)$, $j\in\{0,\dots,p-1\}$; for definition of Hamming's metric $d_H(X,Y)$ and Lee's metric $d_L(X,Y)$ see [12]; $V_p(n,s+1)$ is the maximal linear code in the n-dimensional linear space over $GF(p)$ with Hamming's distance $s+1$ [12] and $V_p^{\perp}(n,s+1)=\{\tau=(\tau_0,\dots,\tau_{n-1})|\bigoplus_{i=0}^{n-1}\tau_i x_i=0$ for all $(x_0,\dots,x_{n-1})\in V_p(n,s+1)\}$.

3. ERROR DETECTING AND CORRECTING CAPABILITY OF SYSTEMS OF LINEAR CHECKS.

Let there be a system of k checks, constructed in accordance with Theorem 1 for a given channel f

$$a_j \circledast f=\varphi_j + Q_j\ ;\ j = 1,2,\dots,k\ . \qquad (11)$$

($a_j(t)=1$ iff $t\in G_j$, G_j is a normal subgroup in G, $|G_j| > 1$.)

Definition 5.

A system of checks (11) is said to be orthogonal if $G_j\cap G_r = \{I\}$ ($j\neq r$; $j,r = 1,2,\dots,k$). (An analogous definition is used in the theory of threshold decoding for error-correcting codes [12].)

By the multiplicity of an error e we mean $\|e\|$. In a channel $f:G\to C$ this definition is natural if the

Table 1
Linear checks for some important computation channels

no	Channel	Definition of function	Check	Complexity
1	Counter	$f(X)=\sum_{i=0}^{n-1} x_i$	$f(X)+f(X\oplus\mathbb{1})=n$	2
2	Up and down Counter	$f(X,Y)=\sum_{i=0}^{n-1} x_i-\sum_{i=0}^{n-1} y_i$	$f(X,Y)+f(X\oplus\mathbb{1},Y\oplus\mathbb{1})=0$	2
3	Comparator	$f(X,Y)=\begin{cases}1, X>Y\\ 0, X=Y\\ -1, X<Y\end{cases}$	$f(X,Y)+f(X\oplus\mathbb{1},Y\oplus\mathbb{1})=0$	2
4	Adder	$f(X,Y)=X+Y$	$f(X,Y)+f(X\oplus\mathbb{1},Y\oplus\mathbb{1})=2(2^n-1)$	2
5	Subtractor	$f(X,Y)=X-Y$	$f(X,Y)+f(X\oplus\mathbb{1},Y\oplus\mathbb{1})=0$	2
6	Multiplier	$f(X,Y)=X\cdot Y$	$f(X,Y)+f(X\oplus\mathbb{1},Y)+f(X,Y\oplus\mathbb{1})+f(X\oplus\mathbb{1},Y\oplus\mathbb{1})=(2^n-1)^2$	4
7	Computation of Hamming's metric	$f(X,Y)=d_H(X,Y)$	$\sum_{j=0}^{p-1} f(X\oplus J,Y)=n(p-1)$	p
8	Computation of Lee's metric	$f(X,Y)=d_L(X,Y)$	$\sum_{j=0}^{p-1} f(X\oplus J,Y)=\frac{n}{4}\left(p^2-\frac{1+(-1)^{p+1}}{2}\right)$	p
9	Quadratic form computation	$f(X,Y)=\sum_{u,v=0}^{n-1} a_{uv}x_u y_v$	$\sum_{j_1,j_2=0}^{p-1} f(X\oplus J_1,Y\oplus J_2)=p^2(p-1)^2 2^{-2}\sum_{u,v=0}^{n-1} a_{uv}$	p^2
10	Polynomial Computation	$f(X)=\sum_{i=0}^{s} a_i X^i$	$\sum_{\tau\in V_p^{\perp}(n,s+1)} f(X\oplus\tau)=\lvert V_p(n,s+1)\rvert^{-1}\sum_{X\in G} f(X)$	$\frac{p^n}{\lvert V_p(n,s+1)\rvert}$

errors in computing $f(t)$ are independent for different t - as, for example, in the case $f(t)$ is information stored in a memory cell with address t.

The following theorem solves the problem of maximal multiplicity of errors detected or corrected by a system (11) of k orthogonal checks in the case of memoryless decoding (see Def. 2).

Theorem 3.

For any $f:G \to C$ and any orthogonal system of k checks, we have for memoryless decoding:
(i) All errors with multiplicity at most k are detected and all those with multiplicity at most $[\frac{k}{2}]$ are corrected;
(ii) There exist errors with multiplicity $k+1$, $[\frac{k}{2}]+1$, which are not detected and not corrected, respectively.
(Here $[\frac{k}{2}]$ is the greatest integer $\leq \frac{k}{2}$.)

Theorem 3 and Definition 1 yield a method for error correction by memoryless decoding, analogous to the majority logic approach in error-correcting codes [12]. Let $k = 2\ell+1$ and $\|e\| \leq \ell$; then, for any $t \in G$, there exist $i_1,\dots,i_{\ell+1}$ such that $S_{i_1}^{(e)}(t)=\dots=S_{i_{\ell+1}}^{(e)}(t)=e(t)$. We thus have a simple means of error correction by the "*majority rule*" for a syndrome-vector $(S_1^{(e)}(t),\dots,S_k^{(e)}(t))$.

In the parallel case of memory-aided decoding, let $\lambda=(\lambda_1,\dots,\lambda_k)\in\{0,1\}^k$ and $\lambda_j t = \begin{cases} t, & \lambda_j = 1 \\ I, & \lambda_j = 0 \end{cases}$. For a system (11) of k orthogonal checks we denote $M(\lambda)=\{t\in G \mid t=\bigodot_{j=1}^{k} \lambda_j t_j,\ t_j \neq I, t_j \in G_j\}$. Suppose

$$M(\lambda)\cap M(\lambda') = \emptyset \qquad (12)$$

($\emptyset$ empty set; $\lambda\neq\lambda'$; $\lambda,\lambda'\in\{0,1\}^k$).

(Note that from (12) we have $k \leq \log_2 |G|$.)

Theorem 4.

For any $f : G \to C$ and any orthogonal system of k checks satisfying (12) we have for memory-aided decoding
(i) All errors with multiplicity at most 2^k-1 are detected, and all those with multiplicity at most $2^{k-1}-1$ are corrected.
(ii) There exist errors with multiplicity 2^k, 2^{k-1}, which are not detected and not corrected respectively.

Corollary 1.

Let, for a given system (11) of k orthogonal checks satisfying (12), $F = \{f \mid a_j \circledast f = \varphi_j + Q_j\ (j=1,2,\dots,k)\}$. Then for any $f_1, f_2 \in F$, $\|f_1-f_2\|\geq 2^k$.

Thus, any system of k orthogonal checks defines a code with Hamming distance 2^k.

In conclusion, Theorems 3 and 4 indicate that the error detecting and correcting capability of a system of orthogonal checks is independent of the structure of the original group G, and increases exponentially when resorting to memory-aided decoding.

4. INPUT-ERROR CORRECTION IN COMPUTATION CHANNELS

In this section we consider errors in an input signal $t\in G$ for a channel $f(t)$. These are introduced by errors in a message generator or in data transmission between the latter and a computation channel.

Definition 6.

By an input error for a channel $f:G\to C$ we mean any ordered pair $(t_1,t_2)\in G\times G (t_1\neq t_2)$. An error (t_1,t_2) is corrected by a channel iff $f(t_1)=f(t_2)$.

Let $\rho(.,.)$ be a metric on G such th $\rho(t_1 \ominus \tau, t_2 \ominus \tau)=\rho(t_1,t_2)$ for any $\tau,t_1,t_2\in$ (If, for example, G is a group of p-ar vectors, ρ may be the Hamming or Lee metric [12].) By multiplicity of an error (t_1,t_2) we mean $\rho(t_1,t_2)$.

Let $N_f(\ell)$ be a number of errors with multiplicity at most ℓ, corrected by a channel f. Set $f_q(t)=\delta_{f(t),q}$, then by the Wiener-Khinchine theorem for G (see e.g.,[3]) we have

$$N_f(\ell) = \sum_{0<\rho(I,\tau)\leq\ell} \sum_q N_{f_q}(\ell,\tau)= \qquad (13)$$
$$\sum_{0<\rho(I,\tau)\leq\ell} \sum_q (F^{-1}(d_\omega^{-1}|G|\hat{f}_q^*(\omega)\hat{f}_q(\omega)))(\tau$$

Here F^{-1} is the inverse Fourier transform (6) over G and $\hat{f}_q^*(\omega)$ the complex conjugate of the matrix $\hat{f}_q(\omega)$. Formul (13) in conjunction with the algorith of the fast Fourier transform over G[5,6] yields a simple method for analysis of the error-correcting capabilit $N_f(\ell)$ with reference to input errors. (Such a method is useful when the number of different values of f is relatively small; in the case $G = \prod_{j=1}^{m} G_j$, the number of elementary operations required for determining $N_{f_q}(\ell,\tau)$ is $2|G|\sum_{j=1}^{m}|G_j|+|G|$ and the corresponding number of required memory cells is $|G|$.)

The lower bound for the error-correcting capability is estimated as foll Let $V_t(r)=\{\zeta \mid \rho(t,\zeta)\leq r\}$, $V(r)=|V_t(r)|$ for any $t\in G$,

$W(r)=\max_{t\neq\zeta}|V_t(r)\cap V_\zeta(r)|$ and $N_f=\sum_\ell N_f(\ell)$.

Theorem 5.

Let $F(A)$ be the class of all functions $f:G\rightarrow C$ with at most A different values. Then

(i) $$\min_{f\in F(A)} N_f \leq |G|A^{-1}(|G|-A) \qquad (14)$$

and there exists $f_o\in F(A)$ such that

$N_{f_o}=|G|A^{-1}(|G|-A)$ if A divides $|G|$.

(ii) If $W([0,5\ell])>0$ then for any ℓ

$$\min_{f\in F(A)} N_f(\ell) \geq$$
$$\geq 2A(W([0,5\ell]))^{-1}(|G|A^{-1}V([0,5\ell])-|G|)^{+}, \qquad (15)$$

where $x+ = \begin{cases} x, & x\geq 0 ; \\ 0, & x<0 . \end{cases}$

The bound (15) is useful for small ℓ. For example, if f is a function of a q-valued logic (A=q) and $\ell=2$, we have for the Hamming metric [12]

$V(1)=1+n(q-1)$, $W(1)=q$, and by (15)

$N_f(2)\geq 2q^{n-1}(n-1)(q-1)$

and for $3\leq q<2n$, $n\geq 2$ and Lee metric [12],

$V(1)=1+2n$, $W(1)=\begin{cases}3, & q=3\\ 2, & q>3\end{cases}$,

$$N_f(2)\geq\begin{cases}4\ 3^{n-1}(n-1), & q=3\\ q^n(2n-(q-1)), & q>3\end{cases}$$

As for the overall error-correcting capability (i.e. with reference to both types of errors), we have

Corollary 2.

Let $f:G\rightarrow C$ and ρ a metric on G. Then for any system of k orthogonal checks (11), if

$$|G|(V(\ell_1)-1)- \sum_{0<\rho(I,\tau)\leq\ell_1} \sum_q (F^{-1}(d_\omega^{-1}|G|\hat{f}_q^{*}(\omega)\hat{f}_q(\omega)))(\tau) + \ell_2 \leq \beta(k) \qquad (16)$$

then input errors with multiplicity at most ℓ_1 and channel errors with multiplicity at most ℓ_2 are corrected by memoryless decoding if $\beta(k)=[\frac{k}{2}]$, and by memory-aided decoding if the checks satisfy (12) and $\beta(k)=2^{k-1}-1$.

Note that a less refined but more convenient condition for correcting both input errors with multiplicity at most ℓ_1 and channel errors with multiplicity at most ℓ_2 is obtainable from corollary 2 by (13) and (15).

REFERENCES

[1] D.C. Opferman, N.T. Tsao-Wu, On class of rearrangeable switching networks, B.S.T.J., 50, no. 5, May 1971, 1579-1618.

[2] V.E. Benes, Optimal rearrangeable multistage connecting networks, B.S.T.J., 43, no. 4, Part 2, July 1964, 1641-1656.

[3] M.G. Karpovsky, E.A. Trachtenberg, Some optimization problem for convolution systems over finite groups, (to appear in Information and Control).

[4] M.G. Karpovsky, Error detection in digital devices and computer programs with the aid of recurrent equations over finite commutative groups IEEE Trans on Comp., C-26, no. 3, Mar. 1977.

[5] G. Apple, and P. Wintz, Calculation of Fourier transforms on finite Abelian groups, IEEE Trans., IT-16, 1970, 233-236.

[6] M.G. Karpovsky, Fast Fourier transforms on finite non-Abelian groups, (to appear in IEEE Trans. on Comp.).

[7] M.G. Karpovsky, E.S. Moskalev, Realization of a system of logical functions by means of an expansion in orthogonal series, Automat. and Remote Control, vol. 28, 1967, 1921-1932, (Translated from: Avtomatika i Telemekhanika, no.12, 1967 119-129.

[8] M.G. Karpovsky, Finite orthogonal series in the design of digital devices, John Wiley, New York, 1976.

[9] J. Pearl, Optimal dyadic models of time-invariant systems, IEEE Trans., C-24, 1975, 598-603.

[10] M.G. Karpovsky, Harmonic analysis over finite commutative groups in linearization problems for systems of logical functions, Information and Control, vol. 33, 142-165, 1977.

[11] L. Dornhoff, Group representation theory, Marcel Dekker, New York, 1971.

[12] E.R. Berlekamp, Algebraic coding theory, McGraw-Hill, New York, 1968.

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

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

$|H_j|$ is a power of a prime number, the group operation is componentwise addition mod $|H_j|$, $j = 1, \ldots, n$. Let μ be the least common multiple of $|H_1|, \ldots, |H_n|$ 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., $\omega = (\omega_1, \ldots, \omega_n)$, $\omega_j \in \{0, 1, \ldots, |H_j| - 1\}$ and we have

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

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

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

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

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

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

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

A subset $\Omega \subset \hat{G}$ is said to be closed (notation $\Omega = \bar{\Omega}$) if for any $\omega \notin \Omega$ we have $\Omega^\perp \not\subset$ Kern ω. 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 $f(t) = t^2 - 170t - 35$, $t \in \{0, \ldots, 2^8 - 1\}$ 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 $t = (t_1, ..., t_8)$, $t_j \in \{0, 1\}$. Then $f: C_2^8 \to C$ 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 $f = f^{(n)}$ $\hat{f} = f^{(n)}$ 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

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

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

(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

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

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

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

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

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

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

By (6)

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

If $\omega \in \bar{\Omega}$, then $\delta_{\Omega^\perp}(\omega) = d_\omega / |G| \, |\bar{\Omega}^\perp| \, E$, (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 $\omega \notin \bar{\Omega}$

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

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

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

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 $f: G \rightarrow K$ depends only on the complexity $\| \delta_H \| = \sum_{\zeta \in G} \delta_H(\zeta)$ of the function $\delta_H: G \rightarrow \{0, 1\}$.

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

1. For the given $f: G \rightarrow K$, compute by (6) or by (9), (11) $\hat{f}$.
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 $\gamma_{\text{opt}} \in K$, $\tau_{\text{opt}} \in G$, $\bar{\Omega}_{\text{opt}} \subseteq \hat{G}$ from the condition

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

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

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

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 $\operatorname{Im} f\, C'N$ 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 $f_1: C_2 \times C_3 \to GF(11)$ 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 $f_1(\omega)$ 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

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

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

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

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

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

(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 $f(t) = t^2 - 170 - 35$, $f:$ $C_2^8 \rightarrow C$ from the Example 1 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 $f(t) =$ $t^2 - 170t - 35$: $\sum_{\tau \in H_1} f(t \text{ W } \tau) = 120$ (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 $f:$ $G \rightarrow K$. 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 $f: G \rightarrow K$ 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 $\omega = (\omega_1, ..., \omega_{j-1}, 0, \omega_{j+1}, ..., \omega_n)$,

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

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 $\{f^{(0)}, ..., f^{(s-1)}\}, f^{(j)} \colon G \to K$ $(j = 0, 1, ..., s-1)$. Let $G^{(I)}$ be come group with s elements. The system $\{f^{(0)}, ..., f^{(s-1)}\}$ may then be considered as a computation channel $f \colon G^{(I)} \times G \to K$ over the group $G^{(I)} \times G$, and the methods described in this section may be made of use in finding the checks for f (and consequently for the given system $\{f^{(0)}, ..., f^{(s-1)}\}$). In this connection we have an apparently quite difficult problem of optimal selection of a group $G^{(I)}$ of the given order $s = |G^{(I)}|$ 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 $S_j^{(e)}$ $G \to K_j$ defined as:

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

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

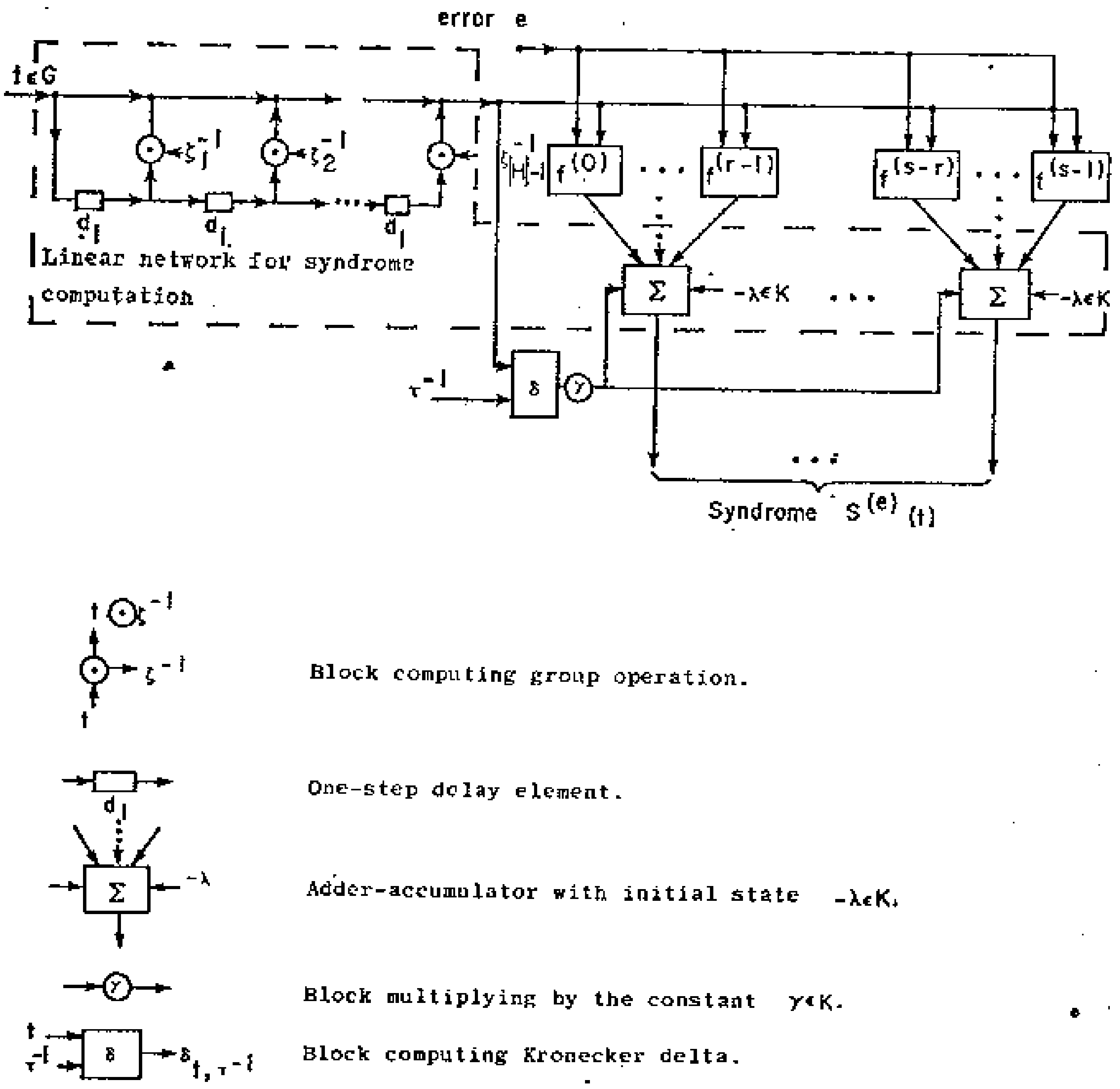

FIG. 1. Network implementation of one check for the system $\{f^{(0)},\ldots,f^{(s-1)}\}$.

$s - 1$). We consider $\{f^{(j)}\}$ as a function $f: G^{(l)} \times G \rightarrow K$, 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

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

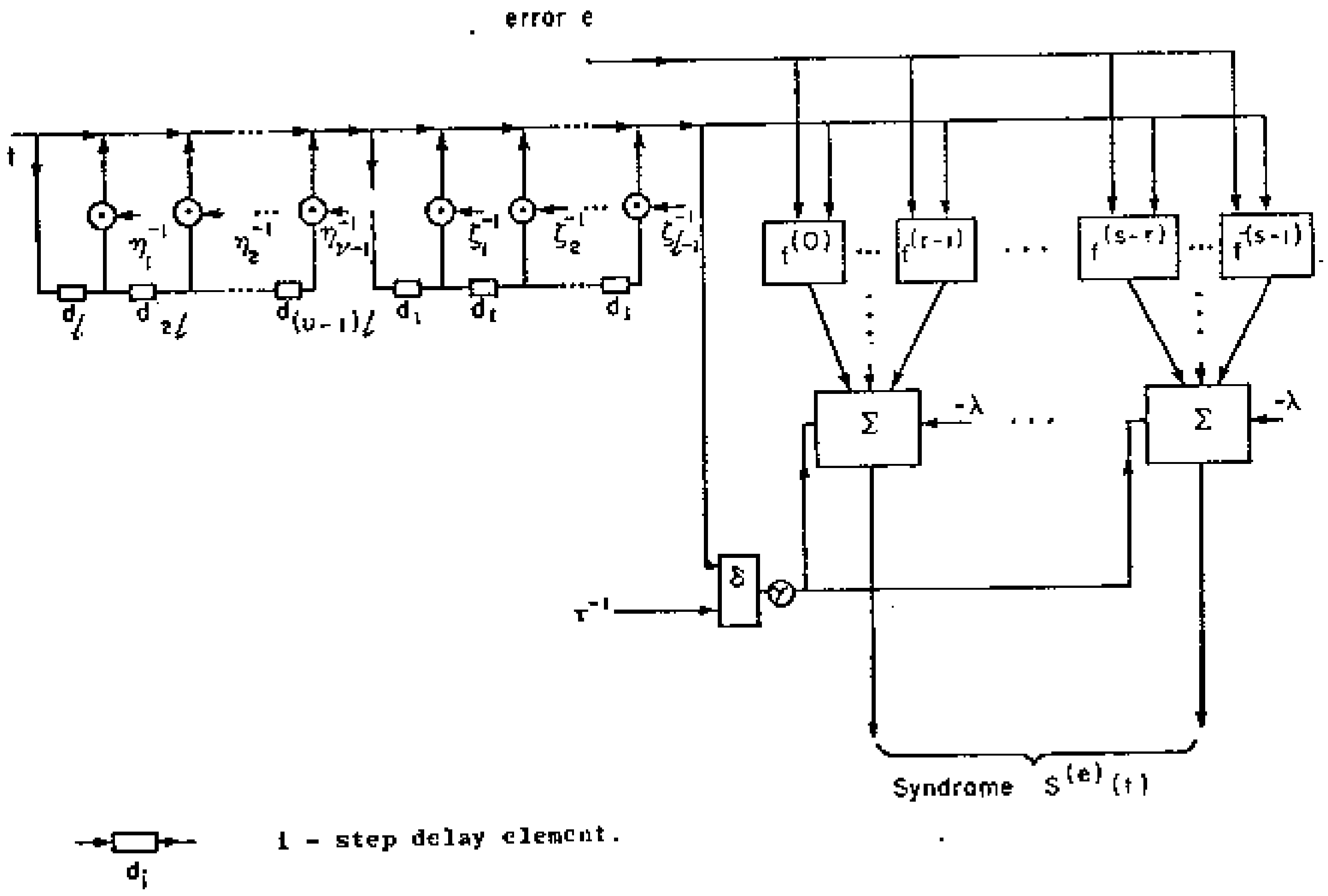

FIG. 2. Network implementation of a check for channel $f = \{f^{(0)},..., f^{(s-1)}\}$ in case H contains the subgroup $H' = \{0, \zeta_1 ,..., \zeta_{l-1}\}$.

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.

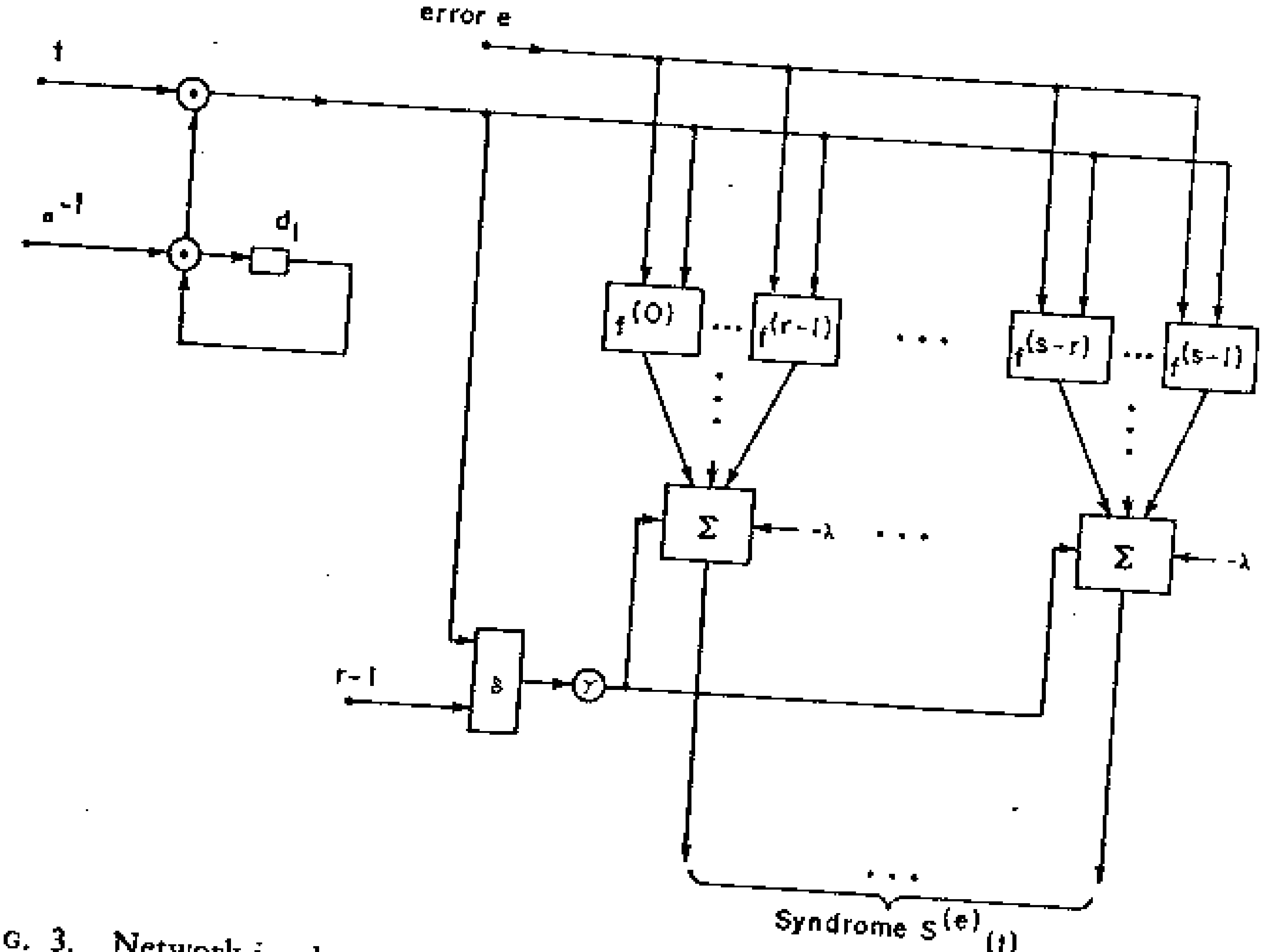

FIG. 3. Network implementation of channel $f = \{f^{(0)},..., f^{(s-1)}\}$ in case of the check, generated by the cyclic subgroup with generator α.

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 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, $| H_j | > 1$, $\operatorname{Im} \varphi_j \subseteq \bigcap_{j=1}^{m} K_j$ 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

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

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

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

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

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

(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* $f: G \rightarrow \bigcap_{j=1}^{m} K_j$ *and any system of m checks* $\delta_{H_j} \circledast f = \varphi_j + \lambda_j$ $(j = 1,..., m)$ *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 $\sigma = (\sigma_1, ..., \sigma_m)$ $(\sigma_j \in \{0, 1\})$ 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 $\sigma = (0,..., 0)$. 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 $\| \sigma' \| = l$ $(l = 1,..., m - 1)$ 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 $(i \in \{1, 2,..., m\})$ 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 $t \in G$, $j \in \{1, 2,..., m\}$ 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 $t_j \in H_j$ $(t_j \neq 0)$, $j = 1,..., m$ and set

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

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

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

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

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

(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)

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

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)

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

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 $\sum_{\tau\in H_i} f(t \mathrm{W} \tau) = 120$ $(i = 1, 2)$, 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 $f \in F$ $(t = 0, 1,..., g - 1)$.

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

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 $\psi \colon G \to K$ $f \circledast \Psi \in F$, $\psi \circledast f \in F$ 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.

OFFERMAN, 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