FUNCTIONS WITH FLAT AUTOCORRELATION AND THEIR GENERALIZATIONS

M.G. Karpovsky, Senior Member IEEE and P. Nagvajara
Research Laboratory for Design and Testing of
Computer and Communication Systems
Department of Electrical, Computer and System Engineering
Boston University
44 Cummington Street, Boston, Massachusetts 02215, USA.

Abstract

Several new constructions for functions with flat autocorrelati presented. Correlation functions considered in this paper are define respect to p-adic ($p \geq 2$) shifts (vector additions modulo p) of variabl show that the total autocorrelation function for a function f(x), (f mapping from an n-dimensional vector space V_n over GF(q) onto GF(q), is flat (invariant for any shift of the space) iff its maxima are over all possible mappings {f}. We construct a class of functions f: GF(q) → GF(q) with a flat total autocorrelation by quadratic form GF(q). Moreover, the autocorrelation function for the characte function $f_i(x) \in \{0,1\}$, $f_i(x) \triangleq 1$ iff $f(x)=i$, $i \in GF(x)$, is also shown asymptotically flat as $n \to \infty$. Applications of functions with autocorrelation to compression of test responses and error-detecting for channels with unknown statistics of errors will be described.

1 Introduction

A function f(x) is "bent" iff $|\{x \mid f(x)=f(x+e)\}|$ is constant (flat) fo $e \neq 0$. The terminology follows from the fact that shifts of linear sub result in either their cosets or subspaces themselves, hence, in this bent functions are the furthest functions from being linear [1]. In paper we will confine ourselves to the shifts of function with respe vector additions modulo p (p-adic shifts $p \geq 2$). Similar results constructing bent functions with respect to cyclic shifts may be fou [9-11].

Two major results concerning the constructions of q-ary bent functio binary asymptotically bent functions are presented. Applications of results in data compression for VLSI testing and error-detecting codes be described. In Section 1 we will define autocorrelation for functions, and show the equivalence between constant autocorre functions and minimum maxima of autocorrelation.

1.1 Definition

Autocorrelation functions for a q-ary function f(x) [2] where $x \in V_n$ GF(q) (V_n denotes n-dimensional vector space) and $f(x) \in GF(q)$, $q=p^s$ defined by

---

[1]This work was supported by the National science Foundation under the Grant DCR-8317763.

$$B_\Sigma(e) \triangleq \sum_i B_i(e) = \sum_i \sum_x f_i(x) f_i(x+e) = |\{x \mid f(x)=f(x+e)\}| . \quad (1)$$

The characteristic function $f_i(x) \in \{0,1\}$ is defined as $f_i(x)=1$ iff $f(x)=i$, $i \in GF(q)$. Note that $x+e$ is defined in V_n over $GF(q)$ and the summations Σ are integer additions. Futhermore, $B_\Sigma(e)$ is the size (cardinality) of the set $\{x \mid f(x)=f(x+e)\}$ and

$$B_i(e) = |\{x \mid f(x)=f(x+e)=i\}|. \quad (2)$$

$B_\Sigma(e)$ and $B_i(e)$ are refered to as the total autocorrelation function and the autocorrelation function of the ith characteristic function $f_i(x)$, respectively.

Functions with flat autocorrelation are important for compression of test responses and error detection for channels with unknown error distributions. For VLSI compression testings $B_\Sigma(e)$ is the number of error-masking events, (x,e): $f(x)=f(x+e)$, for a given error e, where x is a fault-free response. Similarly, for error-detecting codes, $B_i(e)$ is the number of error-masking events, (x,e): $f(x)=f(x+e)=i$, for a given error e, where x is a codeword of the code $C = \{x \mid f(x)=i\}$.

Let us consider the following example illustrating (1).

Example 1. Let $f(x)=uv$, $x=(u,v)$ $u,v \in GF(3)$, that is, $f(x)$: V_2 over $GF(3) \to GF(3)$. Truth tables of $f(x)$, and $f(x+e)$ for $e = (0,1)$, $(1,2)$ and $(2,2)$ and the values of $B_i(e)$, $i=0,1,2$ and $B_\Sigma(e)$ are listed in Table 1(a) and 1(b).

e=(0,0)

x	f	f_0	f_1	f_2
00	0	1	0	0
01	0	1	0	0
02	0	1	0	0
10	0	1	0	0
11	1	0	1	0
12	2	0	0	1
20	0	1	0	0
21	2	0	0	1
22	1	0	1	0

e=(0,1)

x+e	f	f_0	f_1	f_2
01	0	1	0	0
02	0	1	0	0
00	0	1	0	0
11	1	0	1	0
12	2	0	0	1
10	0	1	0	0
21	2	0	0	1
22	1	0	1	0
20	0	1	0	0

e=(1,2)

x+e	f	f_0	f_1	f_2
12	2	0	0	1
10	0	1	0	0
11	1	0	1	0
22	1	0	1	0
20	0	1	0	0
21	2	0	0	1
02	0	1	0	0
00	0	1	0	0
01	0	1	0	0

e=(2,1)

x+e	f	f_0	f_1	f_2
21	2	0	0	1
22	1	0	1	0
20	0	1	0	0
01	0	1	0	0
02	0	1	0	0
00	0	1	0	0
11	1	0	1	0
12	2	0	0	1
10	0	1	0	0

e=(2,2)

x+e	f	f_0	f_1	f_2
22	1	0	1	0
20	0	1	0	0
21	2	0	0	1
02	0	1	0	0
00	0	1	0	0
01	0	1	0	0
12	2	0	0	1
10	0	1	0	0
11	1	0	1	0

Table 1(a). Truth tables for $f(x+e)=(u+t)(v+\tau)$ over GF(3)

e	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
$B_0(e)$	5	3	3	3	2	2	3	2	2
$B_1(e)$	2	0	0	0	1	0	0	0	1
$B_2(e)$	2	0	0	0	0	1	0	1	0
$B_\Sigma(e)$	9	3	3	3	3	3	3	3	3

Table 1(b). Values of Autocorrelation functions

Theorem 1

$B_\Sigma(e)$, $e \neq 0$, is constant (not equal to q^n) iff $B_\Sigma(e) = q^{n-1}$. □

Proof

By summing both sides of (1) over all $e \neq 0$, together with the fact that

$$\sum_{e \neq 0} B_i(e) = \sum_{e \neq 0} \sum_{x} f_i(x) f_i(x+e) = B_i(0)\,(B_i(0)-1), \qquad (3)$$

((3) is readily verified by interchanging the summations, for example, see Table 1(b)). Thus we have

$$Q \triangleq \max_{e \neq 0} B_\Sigma(e) \geq \left\lceil (q^n-1)^{-1} \sum_{i} B_i(0)\,(B_i(0)-1) \right\rceil . \qquad (4)$$

Minimization of (4) over a set of all possible mappings $\{f\}$ with the constraint

$$\sum_{i} B_i(0) = q^n, \qquad (5)$$

results in:

$$Q^* \triangleq \min_{\{f\}} \max_{e \neq 0} B_\Sigma(e) \geq q^{n-1}. \qquad (6)$$

Therefore, the equality in (6) holds iff $B_\Sigma(e) = q^{n-1}$ for all $e \neq 0$. □

1.2 Binary Bent Functions

For the case of binary bent functions $f(x) \in \{0,1\}$ we have the following relationship between $B_\Sigma(e)$, $B_1(e)$ and $B_0(e)$. Since for $f(x) \in \{0,1\}$ and $f_0(x)$ can be writen as $f_0(e) = 1 - f_1(0)$ (arithmatic minus), (1) becomes

$$B_\Sigma(e) = B_0(e) + B_1(e) = q^n - 2B_1(0) + 2B_1(e). \qquad (7)$$

Generalized binary bent functions can be defined as $f(x) \in \{0,1\}$, f: V_n over $GF(q)$, $q=p^s$, $\rightarrow \{0,1\}$, and characterized by the dichotomy induced by f on the space into $C_i = \{x \mid f(x)=i\}$, $i=0,1$, such that $B_\Sigma(e)=q^{n-1}$.

Let us consider the following example to show the lower bound on Q and the uniqueness of $|C_i| = B_i(0)$ for the case of binary bent functions with $p=2$.

Example 2. Consider $f(x) \in \{0,1\}$ where $x \in V_n$ over $GF(2)$. From (4) and (5)

$$Q^* = \min_{\{f\}} Q = \min_{\{y\}} (2^n-1)^{-1} \beta(y), \quad y \triangleq B_1(0) \text{ and } \beta(y) = 2y^2 - 2^{n+1}y + 2^n(2^n-1). \qquad (8)$$

One can see that $\beta(y) \geq \beta(2^{n-1})$, however, 2^n-1 does not divide $\beta(2^{n-1})$. Moreover, $\beta(2^{n-1}-\Delta) = \beta(2^{n-1}+\Delta)$. Let $y = 2^{n-1}+\Delta$, then we have, $\beta(\Delta) = 2\Delta^2 + 2^n(2^{n-1}-1)$. By letting $\Delta=0$, we have, $Q^* \geq \lceil 2^{n-1} - 2^{n-1}(2^n-1)^{-1} \rceil = 2^{n-1}$ (see (6)) which implies $\Delta = \pm 2^{n/2-1}$. Since $\beta(y)$ is convex, binary bent functions exist only for $B_i(0) = 2^{n-1}+2^{n/2-1}$, $2^{n-1}-2^{n/2-1}$, $i \in \{0,1\}$. □

Binary bent functions [1,2,7-10] f(x) (f: V_n over GF(2) $\rightarrow$ {0,1}) can be constructed by the following formula

$$f(x) = f(u,v) = \langle u, \pi(v)\rangle + G(u), \tag{9}$$

where $u,v \in V_{n/2}$ over GF(2), $\langle\ ,\ \rangle$ denotes inner product and $\pi(v)$ denotes permutation on components of v.

It is important to note, that n must be even for the existence of f(x) ($x \in V_n$ over GF(q)).

Often [1,2,7-10] $F(x) \triangleq (-1)^{f(x)}$, F: V_n over GF(2) $\rightarrow$ {1,-1}, was considered instead of f: V_n over GF(2) $\rightarrow$ {0,1}. In this case the autocorrelation function (1) of F(x) becomes the difference in sizes of the sets $\{x \mid f(x)=f(x+e)\}$ and $\{x \mid f(x) \neq f(x+e)\}$. Moreover, one have for the Walsh-Hadamard coefficients of F(x), $\hat{F}(\omega)=\pm 2^{n/2}$ for all ω. The relation between the autocorrelation function of F(x) to $B_\Sigma(e)$ is given by

$$\sum_x F(x)F(x+e) = 2^n - 2B_\Sigma(e). \tag{10}$$

2 Q-Ary Bent Functions

A construction of q-ary bent function defined by $B_\Sigma(e) = q^{n-1}$ is given in the following theorem.

Theorem 2

For
$$f(x) = f(u,v) = \langle u,v\rangle, \tag{11}$$

where $f(x) \in GF(q)$, $x \in V_n$ over GF(q), $q=p^s$, $u,v \in V_{n/2}$ over GF(q), we have $B_\Sigma(e) = |\{x \mid f(x)=f(x+e)\}| = q^{n-1}$ for all $e \neq 0$. □

The function $f(x) = uv$, $x \in V_2$ over GF(3) and $u,v \in V_1$ over GF(3) considered in Example 1 is in fact an example of bent function constructed by (11). Let us consider another example of q-ary bent function of the form given in (11).

Example 3. Let $f(x) = f(u,v) = \langle u,v\rangle$ be defined in $f(x) \in GF(2^3)$, $x \in V_{2m}$ over $GF(2^3)$, $u,v \in V_m$ over $GF(2^3)$. Let $u = (u_0, u_1, \ldots, u_{m-1})$, $v = (v_0, v_1, \ldots, v_{m-1})$, $u_i, v_i \in GF(2^3)$ and the polynomial representations of u_i, v_i are $u_i = u_{2,i}\alpha^2 + u_{1,i}\alpha + u_{0,i}$, $v_i = v_{2,i}\alpha^2 + v_{1,i}\alpha + v_{0,i}$, $u_{j,i}, v_{j,i} \in GF(2)$. Then for the irreducible polynomial used in the construction of $GF(2^3)$ being $\alpha^3 + \alpha + 1$, we have

$$f(x) = u_0v_0+u_1v_1+\ldots+u_{m-1}v_{m-1} = g_2(u,v)\alpha^2 + g_1(u,v)\alpha + g_0(u,v), \tag{12}$$

where
$$g_2(u,v) = g_{2,0}(u_0,v_0) + g_{2,1}(u_1,v_1) + \ldots + g_{2,m-1}(u_{m-1},v_{m-1}),$$
$$g_1(u,v) = g_{1,0}(u_0,v_0) + g_{1,1}(u_1,v_1) + \ldots + g_{1,m-1}(u_{m-1},v_{m-1}),$$
$$g_0(u,v) = g_{0,0}(u_0,v_0) + g_{0,1}(u_1,v_1) + \ldots + g_{0,m-1}(u_{m-1},v_{m-1}),$$

$g_j(u,v), g_{j,i}(u_i,v_i) \in GF(2)$ and

$$g_{2,i}(u_i,v_i) = u_{2,i}v_{2,i} + u_{0,i}v_{2,i} + u_{1,i}v_{1,i} + u_{2,i}v_{0,i},$$

$$g_{1,i}(u_i,v_i) = u_{2,i}v_{2,i} + u_{1,i}v_{2,i} + u_{2,i}v_{1,i} + u_{0,i}v_{1,i} + u_{1,i}v_{0,i},$$

$$g_{0,i}(u_i,v_i) = u_{1,i}v_{2,i} + u_{2,i}v_{1,i} + u_{0,i}v_{0,i}.$$

The autocorrelation function of $f(x)$, $B_\Sigma(e) = q^{n-1} = 2^{6m-3}$, for all $e \neq 0$, implies that

$$B_\Sigma(e) = |\{x \mid f(x)=f(x+e)\}|$$

$$= |\{x \mid g_2(x)=g_2(x+e),\ g_1(x)=g_1(x+e),\ g_0(x)=g_0(x+e)\}|. \qquad (13)\ \square$$

From the above example we see that q-ary bent functions constructed by (11) with $q=p^s$ may be veiwed as a system of s p-ary bent functions. This brings us the following theorem.

<u>Theorem</u> 3

Consider

$$f(x) = \langle u,v\rangle = \{g_0(x),\ g_1(x),\ \ldots,\ g_{s-1}(x)\}, \qquad (14)$$

defined in (11) where $g_i(x)$, $i=0,1,\ldots,s-1$ are functions corresponding to the coefficients of the polynomial representation of $f(x)$. Then any system $G(x)$ consisting of r arbitrarily chosen functions from $\{g_i(x), i=0,1,\ldots,s-1\}$ has the property that

$$|\{x \mid G(x)=G(x+e)\}| = p^{2ms-r},\ 1 \le r \le s-1. \qquad (15)\ \square$$

The construction of q-ary bent functions considered in this section, implies a partition of the space V_n over GF(q) into q equivalent classes C_i, $i=0,1,\ldots,q-1$, where

$$C_i = \{x \mid f(u,v)=\langle u,v\rangle=i\},\ i \in GF(q). \qquad (16)$$

Moreover, $B_i(0) = |\{x \mid f(x)=i\}| = |C_i|$, $i=0,1,\ldots,q-1$, such that $B_\Sigma(e)=q^{n-1}$ is unique.

In the next section we will investigate autocorrelation functions $B_i(e)$ of characteristic functions $f_i(u,v)$ and show that $B_i(e)$ is asymptotically bent as $n \to \infty$.

3 <u>Asymptotically Bent Binary Functions</u>

A binary function $f_i(x)$, $f_i: V_n$ over $GF(q) \to \{0,1\}$, $q=p^s$, we are now considering, is the <u>ith</u> characteristic function of $f(u,v) = \langle u,v\rangle$, $u,v \in V_{n/2}$ over GF(q). Let $n=2m$, then

$$f_i(x) \in \{0,1\},\ f_i(x)=1 \text{ iff } f(x)=\langle u,v\rangle=i,\ i \in GF(q),\ u,v \in V_m \text{ over } GF(q). \qquad (17)$$

Theorem 4 [5]

The autocorrelation function of the ith characteristic function

$$B_i(t,\tau) = \left| \{x \mid f(u,v)=f(u+t,v+\tau)=i\} \right|, \quad t,\tau \in V_m \text{ over } GF(q), \tag{18}$$

is given as follows.

(i) For $i \neq 0$,

$$B_i(t,\tau) = \begin{cases} q^{2m-1} - q^{m-1}, & t=\tau=0; \\ q^{2m-2} \pm q^{m-1}, & \text{otherwise.} \end{cases} \tag{19}$$

Moreover, for p=2

$$B_i(t,\tau) = \begin{cases} q^{2m-1} - q^{m-1}, & t=\tau=0; \\ q^{2m-2} + \mu(i,T)q^{m-1}, & \text{otherwise;} \end{cases} \tag{20}$$

where

$$T = \langle t,\tau \rangle \quad \text{and} \quad \mu(i,T) = \begin{cases} 1, & Tr(iT^{-1})=0,\ T \neq 0; \\ -1, & \text{otherwise,} \end{cases} \tag{21}$$

and $Tr(\alpha) = 1+\alpha+\alpha^2+\ldots+\alpha^{2^{s-1}}$, $Tr(\alpha) \in GF(2)$.

(ii) For $i=0$,

$$B_i(t,\tau) = \begin{cases} q^{2m-1} + q^{m-1}, & t=\tau=0; \\ q^{2m-2} + q^{m-1} + \delta_T \cdot (q-2)q^{m-1}, & \text{otherwise,} \end{cases} \tag{22}$$

where $\delta_T \in \{0,1\}$, $\delta_T=1$ iff $T=0$. □

From the above formulae (20) and (22) we have the following theorem.

Theorem 5

The binary function given by (17) is asymptotically bent, that is, as $n \to \infty$,

$$B_i(t,\tau) \sim q^{n-2} \quad \text{for all } (t,\tau) \neq 0, \ i \in GF(q). \tag{23}$$ □

A Lower bound on $\max_{(t,\tau)\neq 0} B_i(t,\tau)$ can also be derived similarly to (5) and it is given by the following theorem.

Theorem 6

$$\max_{(t,\tau)\neq 0} B_i(t,\tau) \geq \begin{cases} 2\left\lceil \dfrac{B_i(0)(B_i(0)-1)}{2(q^n-1)} \right\rceil, & p=2; \\ \left\lceil \dfrac{B_i(0)(B_i(0)-1)}{(q^n-1)} \right\rceil, & p>2. \end{cases} \tag{24}$$

Note that, for p=2, $B_i(t,\tau)$ is an even integer. □

By substituting the values of $B_i(0)$ given in (20) and (22) into (24) one can see that the asymptotical value of $B_i(t,\tau) = q^{2n-2}$ indeed satifies (24) as $n \to \infty$.

In Section 4.2 error-detecting codes constructed from an equivalent class induced by a q-ary bent function will be discussed.

4 Applications of Bent Functions to VLSI Testing and Error-Detection

Bent functions can be applied to error detection in messages transmitted over noisy channels. In particular, we will consider the problem of error (fault) detection/testing for computation channels (VLSI chips) and a design of error-detecting codes for communication Channels. For channels in which the statistics of errors are difficult to model (unknown) or uniformly distributed, a viable strategy for error detection is to provide equal protection against all errors. Hence, bent functions are of insterest because of their constant-autocorrelation property.

4.1 Optimal Compression for VLSI Test Responses

Testing of Very Large Scale Integration (VLSI) chips typically require millions of test patterns [13]. Thus, the problem of excessive size of memory storing the correct (fault-free) responses is encountered. To render this excessive storage problem test responses are compressed into an r-symbol word called "signature" (or "syndrome" as in error-control-codings' terminology). Thus, only the signature of the correct responses is kept as the reference data. By comparing the reference signature and the test responses' signature we decide whether there occured physical failures (faults) causing a malfunction of the device-under-test.

To analyze the performance of the test responses compression scheme, we assume that faults manifest themselves as errors in test responses. (This is guaranteed for the case of exhaustive testing, of course, excluding physical failures in redundant components.) The performance measure for a compressor of test responses is defined in terms of the conditional error-masking probabilities given errors. These probabilities are defined in the following way.

Let x be the fault-free response which is viewed as an n-dimensional vector over q-ary symbols, that is, $x \in V_n$ over GF(q), $q=p^s$ (For most VLSI applications p=2). With the probabilty space of the fault-free responses attained from testing of an ensemble of VLSI devices we can assume equally-likely probabilies for all x. Now, the conditional error-masking probabilties given error vector e, $e \in V_n$ over GF(q), $e \neq 0$, is defined as

$$Q_I(e) \triangleq \left| \{x \mid f(x)=f(x+e)\} \right| q^{-n} = q^{-n} \hat{B}_I(e), \qquad (25)$$

where f(x) is the signature of the fault-free response x and the compression is defined by the mapping f: V_n over GF(q) $\to$ GF(q). Moreover, an error (x,e) is masked iff $f(x)=f(x+e)$.

In the following theorem we summarize the application of q-ary ($q=p^s$) bent function to the compression testing of VLSI devices.

Corollary 1 [3].

Quadratic compressors $G(x) = \{g_0(x), g_1(x), \ldots, g_{r-1}(x)\}$ where $G(x)$ is a subset of $f(x) = \{f_0(x), f_1(x), \ldots, f_{s-1}(x)\} = f(u,v) = \langle u,v\rangle$, $u,v \in V_m$ over $GF(q)$, $f(x) \in GF(q)$, $q=p^s$, $f_i(x) \in GF(p)$, are optimal with respect to the lower bound

$$\min_{\{f\}} \max_{e \neq 0} Q_\Sigma(e) \geq p^{-r}, \quad r \leq s. \tag{26}$$

□

From the above corollary we conclude that for the case when the probabilty distribution of errors in VLSI test responses is difficult to characterize quadratic compressors provide an optimal protection with $Q_\Sigma(e) = p^{-r}$ for all $e \neq 0$ (where r is the size of signature). In other words, the average performance of quadratic compressors

$$Q_{total} = \sum_{e \neq 0} Q_\Sigma(e) \Pr[e \mid e \neq 0] = p^{-r}, \tag{27}$$

is independent of a probabilty distribution of errors $\Pr[e \mid e \neq 0]$.

4.2 Quadratic Codes

In this section we will consider the problem of constructing optimal error-detecting codes for communication channels with unknown errrors characteristics which may arise due to jammings or other modeling uncertainties [15].

Let x be a codeword and $\tilde{x}$ be a received message, possibly corrupted by an error e, $\tilde{x} = x+e$. We define the conditional error-masking probability, given error e $(e \neq 0)$, for the code C as follows

$$Q(e) \triangleq |\{(x,\tilde{x}) \mid \tilde{x}=x+e,\ x,\tilde{x} \in C\}| \cdot |C|^{-1}. \tag{28}$$

Our goal is for a given number of codewords $|C|$ and a block size n, to construct a code such that maxima of Q(e) over all $e \neq 0$ are minimal. In other words, for a given code rate [1] $R=n^{-1}\log_q |C|$ (codewords are blocks of q-ary symbols of length n), construct a code satisfying the minimax criterion on Q(e), that is, $\min_{C \in S_R} \max_{e \neq 0} Q(e)$, where S_R is a set of all codes with rate R.

The following corollaries summarize the definition and parameters of quadratic codes C and show that these codes are asymptotically optimal with respect to the minimax criterion on error detection. (This minimax criterion has been widly used in estimation theory [15,16]).

Corollary 2 [6]

Let for a given $\sigma \in GF(q)$,

$$(u,v) \in C \Leftrightarrow \langle u,v\rangle = \sigma, \tag{29}$$

where a codeword (u,v) is a block q-ary symbols of length n=2m, that is, $u,v \in V_m$ over $GF(q)$, $q=p^s$. Then the number of q-ary information symbols for C is $k = n-1$ and the number q-ary check symbols is $r = 1$. Further, we have for the conditional error-masking probability, given error $e=(t,\tau)$ $(e\neq 0)$,

$$Q(t,\tau) = \left|\{(u,v) \mid \langle u,v\rangle = \langle (u+t),(v+\tau)\rangle = \sigma\}\right| \cdot |C|^{-1} = B_\sigma(t,\tau)B_\sigma(0,0)^{-1}, \quad (30)$$

and the formulae for $|C| = B_\sigma(0,0)$ and $Q(t,\tau)$ are given as follows.

(i) <u>For $\sigma\neq 0$,</u>

$$|C| = q^{2m-1}-q^{m-1}, \quad (31)$$

$$Q(t,\tau) = (q^{2m-2}\pm q^{m-1})(q^{2m-1}-q^{m-1})^{-1} \to q^{-1} \text{ as } n \to \infty, \ (t,\tau)\neq 0. \quad (32)$$

Moreover, for $q=2^s$

$$Q(t,\tau) = (2^{2ms-2s}+\mu(\sigma,T)2^{ms-1})(2^{2ms-s}-2^{ms-s})^{-1} \to 2^{-s} \text{ as } n \to \infty, \quad (33)$$

$(t,\tau)\neq 0$, where $T=\langle t,\tau\rangle$ and $\mu(\sigma,T)\in\{1,-1\}$, $\mu(\sigma,T)=1$ iff $Tr(\sigma T^{-1})=0$, $T\neq 0$.

(ii) <u>For $\sigma=0$,</u>

$$|C| = q^{2m-1}-q^{m-1}+q^m, \quad (34)$$

$$Q(t,\tau) = (q^{2m-2}+q^{m-1}+\delta_T\cdot(q-2)q^{m-1})(q^{2m-1}-q^{m-1}+q^m)^{-1} \to q^{-1} \text{ as } n \to \infty, \quad (35)$$

$(t,\tau)\neq 0$ where $\delta_T\in\{0,1\}$, $\delta_T=1$ iff $T=0$. □

<u>Corollary</u> 3 [5]

The lower bound on the conditional error-masking probability given error e $(e\neq 0)$ is given by

$$\max_{(t,\tau)\neq 0} Q(t,\tau) \geq \begin{cases} \dfrac{2}{|C|}\left[\dfrac{|C|(|C|-1)}{2(q^n-1)}\right], & p=2; \\[2ex] \dfrac{1}{|C|}\left[\dfrac{|C|(|C|-1)}{(q^n-1)}\right], & p>2. \end{cases} \quad (36)$$

Therefore, quadratic codes are asymtotically optimal with respect to (36). □

In summary, quadratic codes provide equal protection against all errors. For these codes a total error-masking probability

$$Q_{total} = \sum_{e\neq 0} Q(e) \Pr[e \mid e\neq 0] \approx q^{-1} \quad (37)$$

is independent on a distribution of errors $\Pr[e \mid e\neq 0]$. Hence, quadratic codes offer a viable alternative for error-detecting for channels with unknown or difficult to model noise characteristics.

We will conclude this section with an example of a quadratic code which also illustrates the encoding and decoding procedures.

<u>Example</u> 4. The quadratic code with the block size $n=4$ and symbols from $GF(2^2)$ where the number of information symbols is $k=3$, the number of redundant symbol is $r=1$ and syndrome $\sigma=1$, $1 \in GF(2^2)$ is presented in Table 2(a). For a codeword (u_0,u_1,v_0,v_1), $u_i,v_i \in GF(2^2)$, v_1 is the redundant symbol if $M_1 \neq 0$ and v_0 is the redundant symbol if $M_1=0$ (redundant symbol is underlined for every codeword shown). Note that $(M_0,M_1)=(u_0,u_1) \neq (0,0)$ since for this example $(u,v) \in C$ iff $\langle u,v \rangle = \sigma = 1$. For this code $|C| = 60$ and the maximum value of $Q(e)$ is 0.3333.

Message M_0,M_1,M_2			Codewords (u_0,u_1,v_0,v_1)			
0	1	0	0	1	0	$\underline{1}$
0	1	1	0	1	1	$\underline{1}$
0	1	α	0	1	α	$\underline{1}$
0	1	α^2	0	1	α^2	$\underline{1}$
0	α	0	0	α	0	$\underline{\alpha^2}$
	⋮				⋮	
1	0	0	1	0	$\underline{1}$	0
1	0	1	1	0	$\underline{1}$	1
1	0	α	1	0	$\underline{1}$	α
1	0	α^2	1	0	$\underline{1}$	α^2
1	1	0	1	0	1	$\underline{1}$
	⋮				⋮	
α^2	α^2	α	α^2	α^2	α	$\underline{0}$
α^2	α^2	α^2	α^2	α^2	α^2	$\underline{1}$

Table 2(a). Example of a Quadratic Code

- $(u_0,u_1,v_0,v_1) \in C \Leftrightarrow \langle (u_0,u_1),(v_0,v_1) \rangle = 1$
- $(u_0,u_1),(v_0,v_1) \in V_2$ over $GF(2^2)$
- $u_i,v_i \in GF(2^2)$

0	0 0
1	0 1
α	1 0
α^2	1 1

Table 2(b). Elements of $GF(2^2)$

5 <u>Conclusion</u>

A theory of bent (flat autocorrelation) functions and their applications to error-detection in computation and communication channels have been presented. Traditionally, bent functions were defined as mapping from n-dimensional vector space over {0,1} onto {0,1} and generally as quadratic forms over GF(2). We have shown that bent functions, which are characterized by their autocorrelation functions being a constant, can also be constructed as mappings from V_n over $GF(q)$ onto $GF(q)$, $q=p^s$. However, these generalized bent functions $f(x)=f(u,v)=\langle u,v \rangle$ (quadratic forms) have only the total autocorrelation functions being constant $B_\Sigma(e) = |\{x \mid f(x)=f(x+e)\}| = q^{n-1}$ for all $e \neq 0$. We have shown further that the autocorrelation function of the characteristic function $f_i(x) \in \{0,1\}$, $f_i(x)=1$ iff $f(x)=i$, $B_i(e)$ is asymptotically constant as $n \to \infty$. Therefore, a class of binary asymptotically bent functions has been developed. Applications of q-ary bent functions to error-detection are justified when the statatistic of errors are unknown. For error detection schemes based on minimax criteria, we have shown that compression of test responses techniques and error-detection codes constructed by bent functions are optimal.

Acknowledgment

The authors would like to thank Dr. Lev B. Levitin of Boston University for many helpful discussions.

References

1. F.J. McWilliams and N.J.A. Sloane, N. J. The Theory of Error-Correcting Codes, North-Holland Publishing Company, 1978.
2. M.G. Karpovsky, Finite Orthogonal Series in The Design of Digital Devices, Halsted Press, John Wiley & Son, Inc., 1976.
3. M.G. Karpovsky and P. Nagvajara, "Optimal time and space compression for VLSI devices," Proc. IEEE International Test Conf., 1987, pp 523-529.
4. ——, "Optimal compression of test responeses," submitted to IEEE Trans. on Computer.
5. ——, "Asymtotically Bent Functions and Optimal Codes for Minimax Criterion on Error-detection," Proc. IEEE 1988 International Symposium on Infomation Theory, Japan.
6. ——, "Optimal codes for minimax criterion on error detection," submitted to IEEE Trans. on Information Theory.
7. O.S. Rothaus, "On 'Bent' functions," J. Comb. Theory, Series 20A, 1976, pp. 300-305.
8. R.L. McFarland, "A Family of difference sets in non-cyclic groups," J. Comb. Theory, Series A15, 1976, pp. 1-10.
9. J.D. Olsen, R.A. Scholtz and L.R. Welch, "Bent-function sequences," IEEE Trans. on Information Theory, Vol. IT-28, No. 6, Nov. 1982, pp. 858-864.
10. A. Lempel and M. Cohn, "Maximal families of bent sequences," IEEE Trans. on Information Theory, Vol. IT-28, No. 6, Nov. 1982, pp. 865-868.
11. ——, "Design of universal test sequences for VLSI," IEEE Trans. on Information Theory, Vol. IT-31, No. 1, Jan. 1985, pp. 10-17.
12. R. Lidl and H. Niederreiter, Finite Fields, Addison Wesley Publishing Company, 1983.
13. J. Savir, G.S. Ditlow and P.H. Bardell, "Random Patterns Testability," IEEE Trans. on Computer, Vol. 33, No. 1, Jan. 1984, pp. 79-89.
14. J.E. Smith, "Measure of effectiveness of fault signature analysis," IEEE, Trans. on Computer., Vol. C-30, No. 6, Jun. 1980, pp. 510-514.
15. S. Verdu and V.H. Poor, "Minimax robust discrete-time matched filters," IEEE Trans. on Commun., Vol. COM-31, No. 2, Feb. 1983, pp. 208-216.
16. H.L. Van Tree, Detection, Estimation, and Modulation Theory, Part 1, John Wiley & Sons, 1968.