ASYMPTOTICALLY BENT FUNCTIONS AND OPTIMAL QUADRATIC CODES

FOR MINIMAX CRITERION ON ERROR DETECTION

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 Cummings Street Boston, Massachusetts 02215

Abstract

We present optimal error-detecting codes for channels which distributions of errors are not known. The characteristic functions of these code are asymptotically bent. That is, for a given block size n and the number of codewords |C|, these codes minimize \( \max_{e \in \mathcal{E}} Q(e) \) where \( Q(e) \) is the conditional error-masking probability given the error pattern \( e \). The codewords are blocks of \( n \) symbols from \( \text{GF}(q) \), where \( q = p^2 \). We have the following parameters associated with the quadratic codes: \( n = 2m, \ |C| = q^{2m-1} - q^{m-1}, \ Q(e) = (q^{2m-2} - q^{m-1}) |C|^{-1} \), \( e \in \mathcal{E} \). Since \( Q(e) = q^{-1} \) for all \( e \in \mathcal{E} \) as \( n \to \infty \), the quadratic codes are asymptotically optimal with respect to the minimax criterion on \( Q(e) \). In other words, the total error-masking probability, \( Q_{\text{total}} = \sum_{e \in \mathcal{E}} Q(e) \text{Pr}[e \in \mathcal{E}] = q^{-1} \), is independent on an error distribution \( \text{Pr}[e \in \mathcal{E}] \).

\(^1\)This work was supported by the National Science Foundation under the Grant DCR-8317763.
Summary

We present a construction of error-detecting codes asymptotically satifying
the lower bound on maxima of the conditional error-masking probability. The
conditional error-masking probabilities for the code \( C \) given errors \( e, (e=0) \), is defined as

\[
Q(e) = \max \left\{ \left| C \right| \left| C^{-1} = B(e) \right| \right. \left. \left| C \right|^{-1} \right\}
\]

where \( B(e) \) is the autocorrelation function for the characteristic function
\( f(x) \) for the code \( C, f(x)=\begin{cases} 0, & x \in C \\text{or} \ x \notin C \end{cases} \), moreover, \( B(0)=\left| C \right| \left( 1 \right) \).

Our problem can be formulated in the following way: For a given code
rate \( R = \frac{n}{n} \log_q \left| C \right| \left( 2 \right) \) (codewords are blocks of \( q \)-ary symbols of length \( n \)),
construct codes based on \( \min \max_{e,0} Q(e) \) where \( S_R \) denotes the set of all codes
\( C \in S_R \) \( e=0 \)
with the rate \( R \).

Consider codes \( C \) defined in \( V_n \) over \( GF(q) \), \( q=p^5 \). The maxima of the
conditional error-masking probabilities given errors \( e, (e=0) \), \( Q(e) \) is
lowerbounded by:

\[
\max_{e,0} Q(e) \geq \begin{cases} \frac{2}{\left| C \right|} \left( \left| C \right| - 1 \right) \left( \frac{1}{2} (q^n - 1) \right) \quad , \quad p = 2; \\
\frac{1}{\left| C \right|} \left( \left| C \right| - 1 \right) \left( \frac{1}{q^n - 1} \right) \quad , \quad p > 2. 
\end{cases}
\]

For the codes \( C \) based on bent \( [1-11] \) functions, \( (u,v) \in C \Rightarrow \langle u,v \rangle = \sigma \), \( u,v \in V_n \) \( GF(2) \), \( \sigma \in GF(2) \), (\( \langle , \rangle \) denotes inner product), the conditional
error-masking probabilities satisfy the lower bound. Unfortunately, in this
case \( Q(e) \) is asymptotically equal to one half as \( n \to \infty \).
We will describe below the asymptotically optimal quadratic codes for wide range of \(|C|\), \(n\) and \(\text{Max } Q(e)\).

Let \(n=2m\), \(u, v \in V_m\) over \(GF(q)\), \(q=p^S\), that is, \(u = (u_0, u_1, \ldots, u_{m-1})\), and \(v = (v_0, v_1, \ldots, v_{m-1})\), where \(u_i, v_i \in GF(q)\). The quadratic code \(C\) is defined as: for a given \(\sigma \in GF(q)\), \((u, v) \in C = (u, v) = \sigma\).

For these codes with \(m \geq 1\) and \(\sigma = 0\), we have for the autocorrelation functions \(B(t, r)\) for the characteristic function for the codes \(f(u, v)\),

\[
B(t, r) = \begin{cases} 
q^{2m-1} - q^{m-1}, & t = r = 0; \\
q^{2m-2} + \mu(\sigma, T)q^{m-1}, & \text{otherwise},
\end{cases}
\]

where \(T = (t, r)\) and \(\mu(\sigma, T) \in \{0, 1\}\). For \(p=2\), \(\mu(\sigma, T) = 1\) iff \(\text{Trace}(\sigma T^{-1}) = 0\), \(T=0\).

For \(m \geq 1\) and \(\sigma = 0\), we have

\[
B(t, r) = \begin{cases} 
q^{2m-1} - q^{m-1} + q^m, & t = r = 0; \\
q^{2m-2} + q^{m-1} + \delta_T(q^{2m-2})q^{m-1}, & \text{otherwise},
\end{cases}
\]

where \(\delta_T \in \{0, 1\}\), \(\delta_T = 0\) iff \(T=0\).

For \(m=1\) and \(\sigma = 0\), \(C\) is defined as: \((u, v) \in C = uv = \sigma\), \(u, v, \sigma \in GF(q)\). In this case we have, \(\text{Max } Q(t, r) = \frac{2}{q-1}\). Moreover, for \(p=2\)

\[
B(t, r) = \begin{cases} 
2^{2^m-1}, & t = r = 0; \\
2, & \text{Trace}(\sigma (tr)^{-1}) = 0, t \neq r; \\
0, & \text{otherwise}.
\end{cases}
\]

The above quadratic codes are nonlinear and nonsystematic. The block size is given by \(n=2m\) symbols over \(GF(p)\). The transmission rate \(n^{-\log_p |C|} = 1\) as \(n \to \infty\). For \(m \geq 1\), the codes are asymptotically optimal as \(n \to \infty\), and we have, \(Q(t, r) = p^{-S}\) for all \((t, r) \neq 0\). For \(m=1\), \(\sigma = 0\) and \(p=2\), the codes are optimal since the minimum value of maxima of \(Q(e)\) \((e = 0)\) is two.
We will describe below the asymptotically optimal quadratic codes for wide range of $|C|$, $n$ and $\text{Max } Q(e)$. 

Let $n = 2m$, $u, v \in V_m$ over $GF(q)$, $q=2^s$, that is, $u = (u_0, u_1, \ldots, u_{m-1})$ and $v = (v_0, v_1, \ldots, v_{m-1})$, where $u_i, v_i \in GF(q)$. The quadratic code $C$ is defined as: for a given $\sigma \in GF(q)$, $(u, v) \in C \iff \langle u, v \rangle = \sigma$.

For these codes with $m \geq 1$ and $\sigma \neq 0$, we have for the autocorrelation function $B(t, r)$ for the characteristic function for the codes $f(u, v)$,

$$B(t, r) = \begin{cases} q^{2m-1} - q^{s-1}, & t = r = 0; \\ q^{2m-2} + \mu(\sigma, T)q^{s-1}, & \text{otherwise,} \end{cases}$$

where $T = \langle t, r \rangle$ and $\mu(\sigma, T) \in \{1, -1\}$. For $p=2$, $\mu(\sigma, T)=1$ iff $\text{Trace}(\sigma^{T^{-1}})=0$, $T=0$.

For $m \geq 1$ and $\sigma = 0$, we have

$$B(t, r) = \begin{cases} q^{2m-1} - q^{s-1} + q^s, & t = r = 0; \\ q^{2m-2} + q^{s-1} + \delta_T(q-2)q^{s-1}, & \text{otherwise,} \end{cases}$$

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

For $m=1$ and $\sigma \neq 0$, $C$ is defined as; $(u, v) \in C \iff \langle u, v \rangle = \sigma$, $u, v, \sigma \in GF(q)$. In this case we have, $\text{Max } Q(t, r) = \frac{2}{q - 1}$. Moreover, for $p=2$

$$B(t, r) = \begin{cases} 2^{s-1}, & t = r = 0; \\ 2, & \text{trace}(\sigma(t)^{-1})=0, t \neq r; \\ 0, & \text{otherwise.} \end{cases}$$

The above quadratic codes are nonlinear and nonsystematic. The block size is given by $n=2ms$ symbols over $GF(p)$. The transmission rate $n^{-1}\log_2 |C| - 1$ is $n - \infty$. For $m \geq 1$, the codes are asymptotically optimal as $n \to \infty$, and we have, $Q(t, r) = p^{s}$ for all $(t, r)=0$. For $m=1$, $\sigma = 0$ and $p=2$, the codes are optimal since the minimum value of maxima of $Q(e)$ ($e=0$) is two.
Let $C^*$ denote modified quadratic-codes defined as a union of $p^{s-t}$ equivalent classes in $V_{2ms}$ over $GF(p)$ induced by $\langle u, v \rangle = \sigma$, $\sigma \in GF(p^s)$. Furthermore, for a given $\sigma^* \in V_T$ over $GF(p)$, $(u, v) \in C^* \iff \langle u, v \rangle \in \Sigma$, where $\Sigma = \{ \sigma = (u, v), u, v \in V_{p^{s-t}} \}$. (\Sigma is a coordinate subspace in $GF(p^s)$ where last $r$ components are assigned to be $\sigma^*$).

Then, for $m > 1$ and $\sigma^* = 0$, we have, $|C^*| = p^{2ms-t} - p^{s-t}$ and the conditional error-masking probability $Q^*(t, r) = p^{-r}$, as $n \to \infty$ for all $t, r > 0$, thus, modified codes are asymptotically optimal.

The codes $C$ and $C^*$ offer a viable alternative for error detection for channels with unknown probability distribution of errors. As one see from the fact that, the total error-masking probability $Q_{total} = \sum_{e=0} Q(e) Pr[e|e=0]$ is independent on a distribution $Pr[e|e=0]$.

Acknowledgement

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

References


