ASYMPTOTICALLY BENT FUNCTIONS AND OPTIMAL QUADRATIC CODES FOR MINIMAX CRITERION ON ERROR DETECTION[1]

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

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 $\max_{e\neq 0} Q(e)$ where Q(e) is the conditional error-masking probability given the error pattern e. The codewords are blocks of n symbols from GF(q), where $q = p^s$. We have the following parameters associated with the quadratic codes; $n = 2m$, $|C| = q^{2m-1-q^{m-1}}$, $Q(e) = (q^{2m-2}\pm q^{m-1})|C|^{-1}$, $e\neq 0$. Since $Q(e) \sim q^{-1}$ for all $e\neq 0$ as $n \to \infty$, the quadratic codes are asymptotically optimal with respect to the minimax criterion on Q(e). In otherwords, the total error-masking probability, $Q_{total} = \sum_{e\neq 0} Q(e)\Pr[e|e\neq 0] = q^{-1}$, is independent on an error distribution $\Pr[e|e\neq 0]$.

---

[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

$$Q(e) \triangleq |\{(x,\tilde{x}) \mid \tilde{x}-x=e, \quad x,\tilde{x} \in C\}||C|^{-1} = B(e)\,|C|^{-1},$$

where B(e) is the autocorrelation function for the characteristic function f(x) for the code C, $f(x)\in\{0,1\}$, $f(x)=1 \Leftrightarrow x\in C$, moreover, $B(0)=|C|$ [1].

Our problem can be formulated in the following way: For a given code rate $R = n^{-1}\log_q|C|$ [2] (codewords are blocks of q-ary symbols of length n), construct codes based on $\underset{C\in S_R}{\text{Min}}\ \underset{e\neq 0}{\text{Max}}\ Q(e)$ where S_R denotes the set of all codes with the rate R.

Consider codes C defined in V_n over GF(q), $q=p^s$. The maxima of the conditional error-masking probabiltities given errors e, (e≠0), Q(e) is lowerbounded by;

$$\underset{e\neq 0}{\text{Max}}\ Q(e) \geq \begin{cases} \dfrac{2}{|C|}\left\lceil \dfrac{|C|(|C|-1)}{2(q^n-1)} \right\rceil, & p=2; \\ \dfrac{1}{|C|}\left\lceil \dfrac{|C|(|C|-1)}{(q^n-1)} \right\rceil, & p>2. \end{cases}$$

For the codes C based on bent [1-11] functions, $(u,v)\in C \Leftrightarrow \langle u,v\rangle=\sigma$, $u,v \in V_n$ over 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 $\max_{e\neq 0} Q(e)$.

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 $\sigma \in GF(q)$, $(u,v) \in C \Leftrightarrow \langle u,v\rangle = \sigma$.

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

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

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

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

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

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

For $m=1$ and $\sigma\neq 0$, C is defined as; $(u,v)\in C \Leftrightarrow uv=\sigma$, $u,v,\sigma \in GF(q)$. In this case we have, $\max_{(t,\tau)\neq 0} Q(t,\tau) = \dfrac{2}{q-1}$. Moreover, for p=2

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

The above quadratic codes are nonlinear and nonsystematic. The block size is given by n=2ms symbols over GF(p). The transmission rate $n^{-1}\log_p|C| \sim 1$ as $n\to\infty$. For $m>1$, the codes are asymptotically optimal as $n\to\infty$, and we have, $Q(t,\tau) \sim p^{-s}$ for all $(t,\tau)\neq 0$. For m=1, $\sigma\neq 0$ and p=2, the codes are optimal since the mimnimum value of maxima of Q(e) ($e\neq 0$) is two.

We will describe below the asymptotically optimal quadratic codes for wide range of $|C|$, n and $\max_{e\neq 0} Q(e)$.

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 $\sigma \in GF(q)$, $(u,v) \in C \Leftrightarrow \langle u,v\rangle = \sigma$.

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

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

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

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

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

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

For $m=1$ and $\sigma\neq 0$, C is defined as; $(u,v)\in C \Leftrightarrow uv=\sigma$, $u,v,\sigma \in GF(q)$. In this case we have, $\max_{(t,\tau)\neq 0} Q(t,\tau) = \dfrac{2}{q-1}$. Moreover, for $p=2$

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

The above quadratic codes are nonlinear and nonsystematic. The block size is given by n=2ms symbols over GF(p). The transmission rate $n^{-1}\log_p|C| - 1$ as $n \to \infty$. For $m>1$, the codes are asymptotically optimal as $n \to \infty$, and we have, $Q(t,\tau) \sim p^{-s}$ for all $(t,\tau)\neq 0$. For $m=1$, $\sigma\neq 0$ and $p=2$, the codes are optimal since the mimnimum value of maxima of Q(e) ($e\neq 0$) is two.

Let C^* denote modified quadratic-codes defined as a union of p^{s-r} equivalent classes in V_{2ms} over GF(p) induced by $\langle u,v\rangle = \sigma$, $\sigma \in GF(p^s)$. Furthermore, for a given $\sigma^* \in V_r$ over GF(p), $(u,v) \in C^* \Leftrightarrow \langle u,v\rangle \in \Sigma$, where $\Sigma \triangleq \{\sigma \mid \sigma=(v,\sigma^*),\ v \in V_{s-r}\}$. ($\Sigma$ is a coordinate subspace in $GF(p^s)$ where last r components are assigned to be σ^*).

Then, for $m>1$ and $\sigma^* \neq 0$, we have, $|C^*| = p^{2ms-r} - p^{ms-r}$ and the conditional error-masking probability $Q^*(t,\tau) \sim p^{-r}$, as $n \to \infty$ for all $(t,\tau) \neq 0$, thus, modified codes are asymtotically 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 $Q_{total} = \sum_{e \neq 0} Q(e) Pr[\, e \,|\, e \neq 0\,]$ is independent on a distribution $Pr[\, e \,|\, e \neq 0\,]$.

Ackknowlegment

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

References

1. M.G. Karpovsky, Finite Orthogonal Series in The Design of Digital Devices, Halsted Press, John Wiley & Son, Inc., 1976.
2. F.J. McWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, 1978.
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 responses," submitted to IEEE Trans. on computer.

5. —— , "Optimal codes for minimax criterion on error detection," submitted to IEEE Trans. on Information Theory.

6. —— , "Functions with flat autocorrelation and their generalizations," to appear in Proc. 3 rd IEEE International workshop on Spectral Techniques, 1988, Dortmund, F.R.G. .

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, 1983.

13. 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.

14. H.L. Van Tree, Detection, Estimation, and Modulation Theory, Part 1, John Wiley & Sons, 1968.