# Extended Welch Inner Product Theorem for Systematic Binary Block Codes

Jia Hou
*School of Electronics & Information, Soochow University, Suzhou, China*
*E-mail:houjiastock@hotmail.com*

Moon Ho Lee
*Institute of Information & Communication, Chonbuk National University, Jeonju, Korea.*
*E-mail: moonho@chonbuk.ac.kr*

### *Abstract*

*A Simple extended Welch inner product theorem is investigated in this paper. Several functions to find the largest possible minimum Hamming distance of the systematic binary block codes are also derived by using the extended Welch inner product theorem. The results will be useful to estimate or design good codes for communications or other information technology.*

## 1. Introduction

In 1974, Welch and his famous paper [1] introduced a great theorem for the inner products among a set of $M$ vectors of length $L$ and norm $1$. In that paper, the author defined the inner products as

$$c_{v\lambda} = \sum_{i=1}^{L} a_i^v \left(a_i^\lambda\right)^* \quad \text{and} \quad c_{\max} = \max_{v \neq \lambda} \left|c_{v\lambda}\right|, \tag{1}$$

where $(\ )^*$ denotes the complex conjugate and the component is with sets of vectors $\{ (a_1^v, ..., a_L^v)$ or $(a_1^\lambda, ..., a_L^\lambda) : v, \lambda = 1, ..., M \}$. Based on these notations and definition, we have the following theorem, which is widely used for coding and sequences design in the communication systems.

***Welch Inner Product Theorem***: Let $k$ be a positive integer. Then we have

$$(c_{\max})^2 \geq \frac{1}{M-1}\left[\frac{M}{\binom{L}{1}} - 1\right], \tag{2}$$

where the maximum inner product value can be bounded.

## 2. Extended Welch theorem

The well known extension of Welch inner product theorem is Welch bound for analyzing the correlations of sequences. Therefore, by considering the period and synchronization, in this case, the cyclic shifts of the sequences should be cared. Thus, the number of the vectors in (2) should be changed from $M$ to $ML$ and then the equation (2) can be rewritten as

$$(c_{\max})^2 \geq \frac{1}{ML-1}\left[\frac{ML}{\binom{L}{1}}-1\right], \tag{3}$$

where the maximum inner product value can be related to the maximum correlation of the sequences. However, we note that the number of the vectors is always larger than the length of the vectors. In the case of $M < L$, the Welch inner product theorem is still not so tighter for the inner product's bound. Therefore, we present two lemmas, which can apply the Welch inner product theorem to calculate the case with $M < L$.

In the case of $M < L$, the Welch inner product theorem is not suitable to calculate the bound, since

$$\frac{1}{M-1}\left[\frac{M}{\binom{L}{1}}-1\right] < 0, \text{ if } M < L. \tag{4}$$

But it is clearly that $(c_{\max})^2$ is always larger than zero, the equation (4) is not useful in this case. Thus, we derive two lemmas extended from the Welch inner product theorem to estimate the tighter bound if $M < L$.

**Lemma 1**: Let $L' = L \bmod M \neq 0$, if $M < L$, the inner product theorem can be rewritten as

$$(c_{\max})^2 \geq \frac{1}{M-1}\left[\frac{M}{L'}-1\right], \quad M > 2. \tag{5}$$

*Proof and Explanation*: As shown in Figure.1 (a), we decompose the $M \times L$ block into two kinds of smaller blocks. One is $M \times M$ block, the other is $M \times L'$ block, where $L' = L \bmod M$. Thus the inner product equation (2) can be represented as

$$\begin{aligned}(c_{\max})^2 &\geq (c_{\max})^2{}_{M\times L'} \\ &= \frac{1}{M-1}\left[\frac{M}{L'}-1\right]\end{aligned}, \text{ by considering } (c_{\max})^2{}_{M\times M} = 0. \tag{6}$$

We now obtain a positive value to denote the inner product's bound.

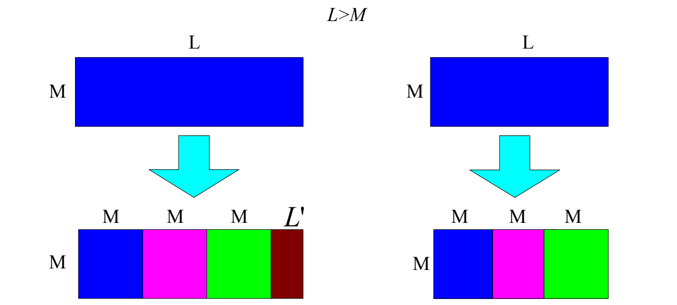
**Lemma 2**: If $L' = L \bmod M = 0$, then the *Lemma 1* can not generalize the inner product's bound. Since $\left.\frac{M}{L'}\right|_{L'=0}$ is not existed. Therefore, we define that

$$(c_{\max})^2 \geq n \times \frac{1}{M-1}\left[\frac{M}{M}-1\right]=0\,,\quad M>2\,. \tag{7}$$

*Proof and Explanation*: As shown in Figure.1 (b), we decompose the $M \times L$ block into only one kind of smaller blocks. Thus the inner product equation (2) can be represented by

$$\begin{aligned}(c_{\max})^2 &\geq (c_{\max})^2_{M\times M} + (c_{\max})^2_{M\times M} + \ldots + (c_{\max})^2_{M\times M} \\ &= \frac{1}{M-1}\left[\frac{M}{M}-1\right] + \frac{1}{M-1}\left[\frac{M}{M}-1\right] + \ldots + \frac{1}{M-1}\left[\frac{M}{M}-1\right] \\ &= 0\,. \end{aligned} \tag{8}$$

We now obtain a non-negative value to denote the inner product's bound.



(a) Block decomposition: $L' = L \bmod M$
$L \bmod M \neq 0$

(b) Block decomposition: $L \bmod M = 0$

**Figure 1**. Block decomposition, if $M < L$.

## 3. Application to Hamming distance estimation for binary block codes

Assuming that the binary code $X$ is $(x_1^v,\ldots,x_L^v)$: $v=1,\ldots,M$, whose length is $L$, and $x_i^v \in \{0,1\}$, $i=1,\ldots,L$, then we can map them to a set of $M$ vectors of length $L$,

$$\hat{x}_i^v = (-1)^{x_i^v}\,,\quad i=1,\ldots,L\text{, and } v=1,\ldots,M\,. \tag{9}$$

As shown in Figure 2, the Hamming distance can be obtained from the inner products based on several computations. First, we denote the Hamming distance of two codewords as

$$d_{v,\lambda} = \sum_{i=1}^{L}(x_i^v \oplus x_i^\lambda)\,,\qquad v,\lambda \in \{1,\ldots,M\}\,, \tag{10}$$

where $\oplus$ is $\bmod 2$ addition. Second, we map $x_i^v$ and $x_i^\lambda$ to the inner products of two vectors $\hat{x}_i^v$ and $\hat{x}_i^\lambda$ by using

$$C_{v,\lambda} = \sum_{i=1}^{L} \hat{x}_i^v \left(\hat{x}_i^\lambda\right)^* = \sum_{i=1}^{L} (-1)^{x_i^v \oplus x_i^\lambda}, \quad v, \lambda \in \{1, \ldots, M\}, \tag{11}$$

where we find that if $x_i^v = x_i^\lambda$, then $x_i^v \oplus x_i^\lambda = 0$, and $\hat{x}_i^v \hat{x}_i^\lambda = 1$; if $x_i^v \neq x_i^\lambda$, then $x_i^v \oplus x_i^\lambda = 1$, and $\hat{x}_i^v \hat{x}_i^\lambda = -1$. In general, we have $C_{v,\lambda} = -dif_{v,\lambda} + sam_{v,\lambda}$, $dif, sam \geq 0$, where $dif_{v,\lambda}$ is the number of $x_i^v \neq x_i^\lambda$, and $sam_{v,\lambda}$ is the number of $x_i^v = x_i^\lambda$. Thus we get $d_{v,\lambda} = dif_{v,\lambda} = sam_{v,\lambda} - C_{v,\lambda}$, $dif_{v,\lambda} + sam_{v,\lambda} = L$, and $d_{v,\lambda} = \dfrac{L - C_{v,\lambda}}{2}$. In addition, the inner product may be rewritten by $\left|C_{v,\lambda}\right|^2 = \left(L - 2d_{v,\lambda}\right)^2$. In practical, we only require the minimum Hamming distance as large as possible. Therefore we can write

$$\min(d_{v,\lambda}) = \frac{L - \max(C_{v,\lambda})}{2}, \text{ if } \max(C_{v,\lambda}) \geq 0. \tag{12}$$

Typically, the systematical linear $(n,k)$ block code gives a parity check matrix [2] as $H = \left\lfloor I_{n-k} \middle| -P^T \right\rfloor$, where $I_{n-k}$ is $(n-k) \times (n-k)$ identity matrix and $P^T$ is the transform of the parity check bits form. It is clearly that $I_{n-k}$ has constant Hamming distance "2", and the parity check form is a $(n-k) \times (k-1)$ block. By applying *Lemma 1* and *Lemma 2*, the distance estimation for this block can be written as

*Case A*: if $(n-k) < (k-1)$, we have

$$\begin{aligned} &\frac{1}{(L')^2} \max_{v \neq \lambda} (L - 2d_{v,\lambda})^2 \geq \frac{1}{M-1} \left[ \frac{M}{L'} - 1 \right] \\ &=> \frac{1}{(L')^2} \max_{v \neq \lambda} ((k-1) - 2d_{v,\lambda})^2 \\ &\geq \frac{1}{(n-k)-1} \left[ \frac{(n-k)}{L'} - 1 \right], \end{aligned} \tag{13}$$

where $L' = (k-1) \bmod (n-k)$. If $(k-1) \bmod (n-k) = 0$, the equation (13) should be changed to

$$\max_{v \neq \lambda} ((k-1) - 2d_{v,\lambda})^2 \geq 0. \tag{14}$$

*Case B*: $(n-k) > (k-1)$, we write that

$$\frac{1}{L^2} \max_{v \neq \lambda} (L - 2d_{v,\lambda})^2 \geq \frac{1}{M-1} \left[ \frac{M}{\binom{L}{1}} - 1 \right]$$

$$=> \frac{1}{(k-1)^2} \max_{v \neq \lambda}((k-1) - 2d_{v,\lambda})^2$$

$$\geq \frac{1}{(n-k)-1} \left[ \frac{(n-k)}{\binom{k-1}{1}} - 1 \right]. \tag{15}$$

*Special Cases*: 1) if $M = 1$, the Hamming distance does not exist; 2) if $M = 2$, the largest Hamming distance can be equal to $L$ , the length of the codewords.

Generally, the possible maximum distance $d_{\max}$ or possible largest minimum Hamming distance of the systematical $H$ matrix for *Case A* and *Case B* can be denoted by

$$d_{\max} = \max(d_{v,\lambda}) + 2, \tag{16}$$

similarly, we also can write the function for the minimum Hamming distance of the systematical generate matrix for binary block codes.

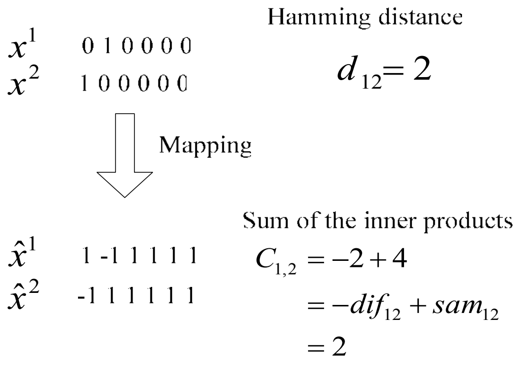


**Figure 2**. Relations between Hamming distance and inner products.

## 4. Conclusion

A simple extension of Welch inner product theorem is investigated. Otherwise, based on the results, we derive some extended lemmas applied to a general Hamming distance estimation for the systematical binary block codes. The contributions will be useful to measure or design good codes for communications system and information technology.

## 5. References

[1] L.R. Welch, “Lower bounds on the maximum cross correlation of signals”, IEEE Trans. On Information Technology, vol. IT-20, no.3, 1974, pp. 397-399.

[2] S.B. Wicker, Error Control Systems for Digital Communication and Storage, Prentice Hall Inc., New York, 1993.

# Authors

Jia Hou, he received his B.S. degree in communication engineering from Wuhan University of Technology in 2000, China, M.S. and Ph.D degree in information & communication from Chonbuk National University, Korea, in 2002 and 2005, respectively. He was the Post-doctoral research fellow in Chonbuk National University, Korea, 2005. He is now the associate professor in school of Electronics & Information, Soochow University, suzhou, China. His main research interests are sequences, CDMA mobile communication systems, error coding, space time signal processing and wireless networking.

Moon Ho Lee, he received his B.S and M.S degrees both in Electrical Engineering, from the Chonbuk National University, Korea, in 1967 and 1976, respectively, and Ph.D degree in electronics engineering from the Chonnam National University in 1984 and the University of Tokyo, Japan, in 1990. From 1970 to 1980, he was a chief engineer with Namyang Moonhwa Broadcasting. Since 1980, he has been a professor in the Department of Information and Communication and a director at the Institute of Information and Communication, both at Chonbuk National University. Dr. Lee is a Registered Telecommunication Professional Engineer and a member of the National Academy of Engineering in Korea. He was the recipient of the paper prize award from the Korean Institute of Communication Science in 1986 as well as in 1987, the Korea Institute of Electronics Engineers in 1987, Chonbuk Province in 1992, The Top Professor of 2001 in Chonbuk National University for his excellent teaching and research, and the commendation of the Prime Minister for inventing the Jacket matrix, in Korea, 2002. His research interests include multidimensional source-channel and space time coding, mobile communication and image processing.