New Lower Bounds on Aperiodic Crosscorrelation of Binary Codes

Vladimir I. Levenshtein

Abstract— **For the minimum aperiodic crosscorrelation $\theta(n, M)$ of binary codes of size M and length n over the alphabet $\{1, -1\}$ there exists the celebrated Welch bound [8]**

$$\theta^2(n, M) \geq \frac{(M-1)n^2}{2Mn - M - 1},$$

which was published in 1974 and has remained in this form up to now [3]. In the paper this bound is strengthened for all $M \geq 4$ and $n \geq 2$. In particular, it is proved that

$$\theta^2(n, M) \geq n - \frac{2n}{\sqrt{3M}}, \quad M \geq 3,$$

and

$$\theta^2(n, M) \geq n - \left\lceil \frac{\pi n}{\sqrt{8M}} \right\rceil, \quad M \geq 5.$$

In the asymptotic process when M tends to infinity as $n \to \infty$, these bounds are twice as large as the Welch bound and coincide with the corresponding asymptotic bound on the square of the minimum periodic crosscorrelation of binary codes. The main idea of the proof is a new sufficient condition for the mean value of a nonnegative definite matrix over the code to be greater than or equal to the average over the whole space. This allows one to take into account weights of cyclic shifts of code vectors and solve the problem of their optimal choice.

Keywords— **binary codes, aperiodic crosscorrelation, Welch bound, inequality on the mean, quadratic forms, Chebyshev polynomials**

I. Introduction

Let E^n be the set of vectors of length n over the alphabet $E = \{1, -1\}$. For any $x = (x_1, ..., x_n) \in E^n$ and $y = (y_1, ..., y_n) \in E^n$ the aperiodic crosscorrelation function $\theta(x, y; l)$ is defined as follows:

$$\theta(x, y; l) = \sum_{j=1}^{n-l} x_j y_{j+l}, \quad l = 0, 1, ..., n-1. \tag{1}$$

Every code $C \subseteq E^n$ is characterized by the maximum aperiodic crosscorrelation magnitude

$$\theta_c(C) = \max\{|\theta(x, y; l)| : x, y \in C,\ x \neq y, l = 0, 1, ..., n-1\},$$

by the maximum out-of-phase aperiodic autocorrelation magnitude

$$\theta_a(C) = \max\{|\theta(x, x; l)| : x \in C, l = 1, ..., n-1\},$$

The author is with the Keldysh Institute for Applied Mathematics, Russian Academy of Science, 125047 Moscow, Russia. The research was supported by the Russian Foundation for the Basic Researh (grant 96-01-00931) and by the Civilian Research and Development Foundation (grant RM1-346). The material in this work was presented in part at the 4th International Symposium on Communication Theory and Applications, Charlotte Mason College, Ambleside, UK, July 13-18, 1997, and at the IEEE International Symposium on Information Theory, MIT, Cambridge, USA, August 16-21, 1998.

and by the value

$$\theta(C) = \max\{\theta_a(C), \theta_c(C)\}$$

which is called the *aperiodic crosscorrelation* of C. The first and, in fact, the only known lower bound on $\theta(C)$ is due to Welch [8]. We shall extend his method by introducing "weights" for shifts of code words and reduce the problem of finding bounds to that of minimization of a quadratic form. The Welch bound is obtained when all the weights are equal. However, a suitable choice of weights allows us to essentially improve this bound if the size of C is 4 or more. We also generalize our approach and give better bounds for the case when the size of C grows as a fixed power of its length.

II. Weighted cyclic shifts

For any vector $z = (z_1, ..., z_N)$ of length N and any integer i, $0 \leq i \leq N-1$, denote by $T_i(z)$ the *right cyclic shift* of z by i positions, that is,

$$T_i(z) = (z_{N-i+1}, ..., z_N, z_1, ..., z_{N-i}).$$

For any $x \in E^n$ let

$$W(x) = \{T_i(x0^{n-1}),\ i = 0, 1, ..., 2n-2\},$$

and for any $C \subseteq E^n$ let

$$W(C) = \bigcup_{x \in C} W(x).$$

Thus, W maps $C \subseteq E^n$ into the set $W(E^n)$ of $(2n-1)2^n$ vectors of length $N = 2n - 1$ over the alphabet $\{1, -1, 0\}$. In particular, for $x = (+, -, +, +)$, $W(x)$ consists of the vectors

$$\begin{array}{ccccccc}
+ & - & + & + & 0 & 0 & 0 \\
0 & + & - & + & + & 0 & 0 \\
0 & 0 & + & - & + & + & 0 \\
0 & 0 & 0 & + & - & + & + \\
+ & 0 & 0 & 0 & + & - & + \\
+ & + & 0 & 0 & 0 & + & - \\
- & + & + & 0 & 0 & 0 & +.
\end{array}$$

To any shift $T_i(x0^{n-1})$, $i = 0, 1, ..., 2n-2$, $x \in E^n$, assign a *weight* w_i (which does not depend on $x \in E^n$) and assume that

$$w_i \geq 0,\ i = 0, 1, ..., 2n-2, \text{ and } \sum_{i=0}^{2n-2} w_i = 1. \tag{2}$$

For any two subsets A and B of E^n define the value

$$F(A, B) :=$$

$$\frac{1}{|A||B|}\sum_{x\in A}\sum_{y\in B}\sum_{s=0}^{2n-2}\sum_{t=0}^{2n-2}|\left\langle T_s(x0^{n-1}),T_t(y0^{n-1})\right\rangle|^2 w_s w_t, \tag{3}$$

where $\langle u,v\rangle$ denotes the usual inner product of vectors u and v. The desired results for a code $C\subseteq E^n$ will be obtained with the help of finding lower and upper bounds on $F(C,C)$. Note that for any $s,t\in\{0,1,...,2n-2\}$ and $x,y\in E^n$, we have

$$|\left\langle T_s(x0^{n-1}),T_t(y0^{n-1})\right\rangle|^2+|\left\langle T_t(x0^{n-1}),T_s(y0^{n-1})\right\rangle|^2$$
$$=|\theta(x,y;l)|^2+|\theta(y,x;l)|^2, \tag{4}$$

where l is equal to

$$l_{s,t,n}=\min\{|t-s|,2n-1-|t-s|\}. \tag{5}$$

Lemma 1: For any code $C\subseteq E^n$ of size M,

$$F(C,C)\le$$
$$\frac{1}{M}\left((n^2-\theta^2(C))\sum_{i=0}^{2n-2}w_i^2+M\theta^2(C)\right). \tag{6}$$

Proof: Considering separately in (3) the cases $x=y,\ s=t$ (in this case $|\left(T_s(x0^{n-1}),T_t(y0^{n-1})\right)|=n$), $x=y,\ s\neq t$, and $x\neq y$ and using (2) we get

$$MF(C,C)\le$$
$$n^2\sum_{i=0}^{2n-2}w_i^2+\theta^2(C)\sum_{s,t=0,s\neq t}^{2n-2}w_s w_t+(M-1)\theta^2(C).$$

This gives (6) taking into account that $\sum_{s,t=0,s\neq t}^{2n-2}w_s w_t=1-\sum_{s=0}^{2n-2}w_s^2$. ■

Lemma 2: For any $x\in E^n$,

$$F(\{x\},E^n)=F(E^n,E^n)=\sum_{s,t=0}^{2n-2}(n-l_{s,t,n})w_s w_t$$

where $l_{s,t,n}$ is defined by (5).

Proof: Using (3) and (4) we have

$$F(\{x\},E^n)$$
$$=\frac{1}{2^n}\sum_{y\in E^n}\sum_{s=0}^{2n-2}\sum_{t=0}^{2n-2}|\left\langle T_s(x0^{n-1}),T_t(y0^{n-1})\right\rangle|^2 w_s w_t$$
$$=\frac{1}{2^{n+1}}\sum_{s=0}^{2n-2}\sum_{t=0}^{2n-2}\sum_{y\in E^n}\left(\theta^2(x,y;l)+\theta^2(y,x;l)\right)w_s w_t$$

with $l=l_{s,t,n}$. From the definition (1) it follows that

$$\theta(x,y;l)=n-l-2d$$

where d is the Hamming distance between vectors $(x_1,...,x_{n-l})$ and $(y_{l+1},...,y_n)$. Therefore,

$$\sum_{y\in E^n}\theta^2(x,y;l)=2^l\sum_{d=0}^{n-l}\binom{n-l}{d}(n-l-2d)^2.$$

Since $2^{-h}\sum_{d=0}^{h}\binom{h}{d}(h-2d)^2=h$ for any positive integer h, we have

$$\frac{1}{2^n}\sum_{y\in E^n}\theta^2(x,y;l)=\frac{1}{2^n}\sum_{y\in E^n}\theta^2(y,x;l)=n-l.$$

This gives the formula for $F(\{x\},E^n)$, which does not depend on $x\in E^n$, and completes the proof. ■

Lemma 3: For any code $C\subseteq E^n$,

$$F(C,C)\ge F(E^n,E^n)=\sum_{s,t=0}^{2n-2}(n-l_{s,t,n})w_s w_t.$$

Proof: Define functions $f_{i,j}(X)$, $i,j=0,1,...,2n-2$, on $W(E^n)$ as follows. If $X=T_s(x0^{n-1})$ where $x\in E^n$ and $X=(u_0,u_1,...,u_{2n-2})$, then $f_{i,j}(X)=u_i u_j w_s$. Using this notation one can rewrite (3) in the following form:

$$F(A,B)=\frac{1}{|A||B|}\sum_{X\in W(A)}\sum_{Y\in W(B)}\sum_{i,j=0}^{2n-2}f_{i,j}(X)f_{i,j}(Y).$$

Let us verify (as in [5]) that for any two subsets A and B of E^n,

$$(F(A,B))^2\le F(A,A)\cdot F(B,B). \tag{7}$$

First change the order of summation and use the Cauchy inequality for sequences:

$$\left|\sum_{X\in W(A)}\sum_{Y\in W(B)}\sum_{i,j=0}^{2n-2}f_{i,j}(X)f_{i,j}(Y)\right|^2$$
$$=\left|\sum_{i,j=0}^{2n-2}\sum_{X\in W(A)}f_{i,j}(X)\sum_{Y\in W(B)}f_{i,j}(Y)\right|^2$$
$$\le\sum_{i,j=0}^{2n-2}\left|\sum_{X\in W(A)}f_{i,j}(X)\right|^2\cdot\sum_{i,j=0}^{2n-2}\left|\sum_{Y\in W(B)}f_{i,j}(Y)\right|^2$$
$$=\sum_{i,j=0}^{2n-2}\sum_{X\in W(A)}f_{i,j}(X)\sum_{Y\in W(A)}f_{i,j}(Y)$$
$$\cdot\sum_{i,j=0}^{2n-2}\sum_{X\in W(B)}f_{i,j}(X)\sum_{Y\in W(B)}f_{i,j}(Y).$$

One more changing the order of summation implies (7). Then we note that for any $A\subseteq E^n$ we have $F(A,E^n)=F(E^n,E^n)$ by Lemma 2. Therefore the use of (7) with $A=C$ and $B=E^n$ completes the proof. ■

The sense of the last statement is connected with sufficient conditions in order that, given a finite set S, the "inequality on the mean" [5], [4] for a nonnegative definite matrix $H(X,Y)$ of order $|S|$ with $X,Y\in S$ to be valid. This means that for any $D\subseteq S$,

$$\frac{1}{|D|^2}\sum_{X\in D}\sum_{Y\in D}H(X,Y)\ge\frac{1}{|S|^2}\sum_{X\in S}\sum_{Y\in S}H(X,Y). \tag{8}$$

It was shown in [5] that (8) is true for any $D \subseteq S$, if $\sum_{Y \in S} H(X,Y)$ does not depend on $X \in S$. However, in the case $S = W(E^n)$ this condition is not satisfied for the nonnegative definite matrix

$$H(X,Y) = \sum_{i,j=0}^{2n-2} f_{i,j}(X) f_{i,j}(Y)$$

considered above and (8) is not true for some $D \subseteq W(E^n)$. Nevertheless, using Lemma 2 we proved that (8) is true for all $D = W(A)$ with $A \subseteq E^n$.

III. Reduction to quadratic form and optimization

For any integer n, $n \geq 2$, number a and vector $\mathbf{w} = (w_0, w_1, ..., w_{2n-2})$, let us consider the quadratic form

$$Q_{2n-1}(\mathbf{w}, a) := a \sum_{i=0}^{2n-2} w_i^2 + \sum_{s,t=0}^{2n-2} l_{s,t,n} w_s w_t \qquad (9)$$

where $l_{s,t,n}$ are defined in (5). Note that $l_{s,t,n} = 0$ when $s = t$. In particular, the matrix $Q_{2n-1}(a)$ of the form $Q_{2n-1}(\mathbf{w}, a)$ for $n = 6$ is given by

$$\begin{array}{ccccccccccc}
a & 1 & 2 & 3 & 4 & 5 & 5 & 4 & 3 & 2 & 1 \\
1 & a & 1 & 2 & 3 & 4 & 5 & 5 & 4 & 3 & 2 \\
2 & 1 & a & 1 & 2 & 3 & 4 & 5 & 5 & 4 & 3 \\
3 & 2 & 1 & a & 1 & 2 & 3 & 4 & 5 & 5 & 4 \\
4 & 3 & 2 & 1 & a & 1 & 2 & 3 & 4 & 5 & 5 \\
5 & 4 & 3 & 2 & 1 & a & 1 & 2 & 3 & 4 & 5 \\
5 & 5 & 4 & 3 & 2 & 1 & a & 1 & 2 & 3 & 4 \\
4 & 5 & 5 & 4 & 3 & 2 & 1 & a & 1 & 2 & 3 \\
3 & 4 & 5 & 5 & 4 & 3 & 2 & 1 & a & 1 & 2 \\
2 & 3 & 4 & 5 & 5 & 4 & 3 & 2 & 1 & a & 1 \\
1 & 2 & 3 & 4 & 5 & 5 & 4 & 3 & 2 & 1 & a.
\end{array}$$

Theorem 1: For any code $C \subseteq E^n$ of size M and $\mathbf{w} = (w_0, w_1, ..., w_{2n-2})$ satisfying (2),

$$\theta^2(C) \geq n - \frac{Q_{2n-1}(\mathbf{w}, n(n-1)/M)}{1 - \frac{1}{M}\sum_{i=0}^{2n-2} w_i^2} \qquad (10)$$

and

$$\theta^2(C) \geq n - Q_{2n-1}(\mathbf{w}, n^2/M). \qquad (11)$$

Proof: Lemmas 1 and 3 show that

$$\theta^2(C)(M - \sum_{i=0}^{2n-2} w_i^2) \geq M \sum_{s,t=0}^{2n-2} (n - l_{s,t,n}) w_s w_t - n^2 \sum_{i=0}^{2n-2} w_i^2.$$

This is equivalent to (10) and implies (11) if $\sum_{i=0}^{2n-2} w_i^2$ will be omitted on the left-hand side. ■

Theorem 1 gives rise to the problem of minimization of the quadratic form $Q_{2n-1}(\mathbf{w}, a)$ under conditions (2). For any positive integer m, let $\mathbf{j}_m = (j_0, j_1, ..., j_{m-1})$ where $j_i = \frac{1}{m}$ for $i = 0, 1, ..., m-1$. For the uniform distribution of the weights, i.e., when $\mathbf{w} = \mathbf{j}_{2n-1}$,

$$Q_{2n-1}(\mathbf{j}_{2n-1}, a) = \frac{a}{2n-1} + \frac{1}{(2n-1)^2} \sum_{s,t=0}^{2n-2} l_{s,t,n}.$$

Since $\sum_{t=0}^{2n-2} l_{s,t,n}$ for $0 \leq s \leq n-1$ equals

$$\sum_{t=0}^{s} (s-t) + \sum_{t=s+1}^{s+n-1} (t-s) + \sum_{t=s+n}^{2n-2} (2n-1-t+s) = (n-1)n \qquad (12)$$

and for $n \leq s \leq 2n-2$ equals

$$\sum_{t=0}^{s-n} (2n-1-s+t) + \sum_{t=s-n+1}^{s-1} (s-t) + \sum_{t=s}^{2n-2} (t-s) = (n-1)n, \qquad (13)$$

we have

$$Q_{2n-1}(\mathbf{j}_{2n-1}, \frac{n(n-1)}{M}) = \frac{n(n-1)}{2n-1}(\frac{1}{M} + 1)$$

and (10) implies the following classical result [8].

Corollary 1 (The Welch bound) For any code $C \subseteq E^n$ of size M,

$$\theta^2(C) \geq \frac{(M-1)n^2}{2Mn - M - 1}. \qquad (14)$$

It is interesting to note that Berlekamp [1, Section 3.14] considered the problem of finding the *maximum* of the quadratic form $Q_{2n-1}(\mathbf{w}, a)$ with $a = 0$ over vectors $\mathbf{w}$ normalized by $\sum_{i=0}^{2n-2} w_i = 1$. This problem arose in connection with obtaining a Plotkin type bound for codes over the alphabet $\{0, 1, ..., 2n-2\}$ in the case of Lee metric. (The matrix of $Q_{2n-1}(0)$ is a distance matrix of the cyclic graph with $2n-1$ vertices.) In particular, he found eigenvalues of $Q_{2n-1}(a)$:

$$\lambda_0 = a + (n-1)n$$

(this corresponds to the eigenvector $\mathbf{j}_{2n-1}$; see (12) and (13)),

$$\lambda_k = a - \frac{1 - (-1)^k \cos \frac{\pi k}{2n-1}}{2 \sin^2 \frac{\pi k}{2n-1}}, \; k = 1, ..., 2n-2,$$

and proved that the quadratic form $Q_{2n-1}(\mathbf{w}, 0)$ is convex on *normalized* vectors $\mathbf{w}$ because $\lambda_k \leq 0$, $k = 1, ..., 2n-2$, for $a = 0$. This implies that the stationary point $\mathbf{j}_{2n-1}$ is the global maximum of $Q_{2n-1}(\mathbf{w}, 0)$ over normalized vectors. Berlekamp's proof also shows that for $\lambda_k \geq 0$, $k = 1, ..., 2n-2$, the stationary point $\mathbf{j}_{2n-1}$ is the global *minimum* of $Q_{2n-1}(\mathbf{w}, a)$ over normalized vectors. In particular, these conditions are satisfied for $a = (n-1)n/2$, $n \geq 2$, since in this case

$$\min_{1 \leq k \leq 2n-2} \lambda_k = \frac{(n-1)n}{2} - \frac{1}{4 \sin^2 \frac{\pi}{2(2n-1)}} \geq 0.$$

Thus, for $M = 1$ and $M = 2$ the Welch bound cannot be improved by the method under consideration. Probably, this is also the case for $M = 3$. However, we shall see that for $M \geq 4$ this bound can be essentially improved with the help of a suitable choice of the weights.

First consider the value of $Q_{2n-1}(\mathbf{w}, a)$ at vectors $\mathbf{w} = (w_0, ..., w_{2n-2})$ such that $w_i = \frac{1}{m}$, $i = 0, 1, ..., m-1$ and $w_i = 0$, $i = m, ..., 2n-2$, for some integer m, $m = 1, ..., 2n-$

2. We will also denote these vectors by $\mathbf{w}(\mathbf{j}_m)$. One can check that $Q_{2n-1}(\mathbf{w}(\mathbf{j}_m), a)$ does not change if we put any $2n-1-m$ (cyclically) consecutive weights to 0, and can only increase for another choice of $2n-1-m$ zero weights. Moreover, it is possible to show that for $n < m \le 2n-1$ the results obtained below cannot be improved. In this connection, for any positive integer m, number a and vector $\mathbf{v} = (v_0, v_1, ..., v_{m-1})$, consider the quadratic form

$$P_m(\mathbf{v}, a) := a \sum_{i=0}^{m-1} v_i^2 + \sum_{s,t=0}^{m-1} |t-s| v_s v_t. \tag{15}$$

In particular, the matrix $P_6(a)$ of the form $P_6(\mathbf{w}, a)$ is given by

$$\begin{matrix} a & 1 & 2 & 3 & 4 & 5 \\ 1 & a & 1 & 2 & 3 & 4 \\ 2 & 1 & a & 1 & 2 & 3 \\ 3 & 2 & 1 & a & 1 & 2 \\ 4 & 3 & 2 & 1 & a & 1 \\ 5 & 4 & 3 & 2 & 1 & a. \end{matrix}$$

Note that if $1 \le m \le n$ and the vector $\mathbf{w}(\mathbf{v})$ is obtained by appending to $\mathbf{v}$ $2n-1-m$ zeros (as before in the case $\mathbf{v} = \mathbf{j}_m$), then

$$Q_{2n-1}(\mathbf{w}(\mathbf{v}), a) = P_m(\mathbf{v}, a). \tag{16}$$

Moreover, if $\mathbf{v} = (v_0, v_1, ..., v_{m-1})$ has the properties

$$v_i \ge 0, \ i = 0, 1, ..., m-1, \text{ and } \sum_{i=0}^{m-1} v_i = 1, \tag{17}$$

then $\mathbf{w}(\mathbf{v})$ satisfies (2). In particular, for any m, $1 \le m \le n$,

$$Q_{2n-1}(\mathbf{w}(\mathbf{j}_m), a) = P_m(\mathbf{j}_m, a) = \frac{a}{m} + \frac{m^2-1}{3m}. \tag{18}$$

Corollary 2: For any code $C \subseteq E^n$ of size M and integer m, $1 \le m \le n$,

$$\theta^2(C) \ge \frac{3nmM - 3n^2 - Mm^2 + M}{3\,(mM-1)}. \tag{19}$$

Proof: This follows from (10) and (18). ■

In particular, for $m = n$ we obtain the bound

$$\theta^2(C) \ge \frac{(2M-3)\,n^2 + M}{3\,(nM-1)}$$

which is stronger than the Welch bound (14) for all $M \ge 4$ and $n \ge 2$.

A further improvement is based on the optimal choice of the parameter m.

Corollary 3: For any code $C \subseteq E^n$ of size M ($M \ge 3$, $n \ge 2$),

$$\theta^2(C) \ge n - \frac{2n}{\sqrt{3M}}. \tag{20}$$

Proof: For $M \ge 3$ there exists an integer m such that $1 \le m \le n$ and $m = \sqrt{\frac{3}{M}}n + \varepsilon$ for some number ε with $|\varepsilon| \le 1$. Using (18) with this m, we get

$$Q_{2n-1}(\mathbf{w}(\mathbf{j}_m), \frac{n^2}{M}) = \frac{6n^2 + 2\sqrt{3M}n\varepsilon + M\varepsilon^2 - M}{3\left(\sqrt{3M}n + M\varepsilon\right)}$$

$$\le \frac{6n^2 + 2\sqrt{3M}n\varepsilon}{3\left(\sqrt{3M}n + M\varepsilon\right)} = \frac{2n}{\sqrt{3M}}.$$

The bound (20) follows from (11). ■

For M sufficiently large, the bound (20) admits a further improvement with by using Lagrange multipliers to find the minimum of the quadratic form $P_m(\mathbf{v}, a)$ under conditions (17). For simplicity we only consider the case of even $m = 2r$.

Let $U_i(z)$, $i = 0, 1, \ldots$, be the Chebyshev polynomials of the second kind (see, for example, [2]) defined as follows:

$$U_i(\cos\theta) = \frac{\sin((i+1)\,\theta)}{\sin\theta}. \tag{21}$$

The polynomials $U_i(z)$, $i = 0, 1, \ldots$, are orthogonal on the interval $[-1, 1]$ with respect to the weight function $(1-z^2)^{\frac{1}{2}}$. They can be uniquely defined by the recurrence

$$U_{i+1}(z) = 2zU_i(z) - U_{i-1}(z), \quad U_{-1}(z) \equiv 0, \quad U_0(z) \equiv 1. \tag{22}$$

Note that polynomials $u_i(z)$, $i = 0, 1, \ldots$, defined by the recurrence

$$u_{i+1}(z) = 2zu_i(z) - u_{i-1}(z), \quad u_{-1}(z) \equiv 1, \quad u_0(z) \equiv 1, \tag{23}$$

are connected with the Chebyshev polynomials as follows

$$u_i(z) = U_i(z) - U_{i-1}(z), \quad i = 0, 1, ... \tag{24}$$

(this follows easily by induction on i).

Theorem 2: Let $C \subseteq E^n$ be a code of size $M \le n^2$, and let φ be defined by $\cos\varphi = 1 - M/n^2$, $0 < \varphi \le \pi/2$. Then for any integer r such that $r\varphi < \pi/2 + \varphi/2$ and $1 \le 2r \le n$,

$$\theta^2(C) \ge n - r - \frac{\sin r\varphi - \sin(r\varphi - \varphi)}{2\,(1-\cos\varphi)\sin r\varphi} + \frac{1}{2}. \tag{25}$$

Proof: For $a = n^2/M$ consider the function $f(\mathbf{v}, \lambda) = P_{2r}(\mathbf{v}, a) - 2\lambda\left(\sum_{i=0}^{2r-1} v_i - 1\right)$ and note that λ and the coordinates of a stationary point $\mathbf{v} = (v_0, ..., v_{2r-1})$, $\sum_{i=0}^{2r-1} v_i = 1$, must satisfy the following system of equations:

$$av_i + \sum_{j=0}^{i-1}(i-j)v_j + \sum_{j=1}^{2r-i-1} jv_{i+j} = \lambda, \ i = 0, ..., 2r-1. \tag{26}$$

Multiply the ith equation by v_i and sum over all i. Since $\sum_{i=0}^{2r-1} v_i = 1$, we obtain $P_{2r}(\mathbf{v}, a) = \lambda$. Our next goal is to find a solution of the system (26) for the additional condition that

$$v_{r-k-1} = v_{r+k}, \quad k = 0, 1, ..., r-1.$$

Toward this end let us introduce new variables

$$y_k = 2v_{r-k-1} = 2v_{r+k} \quad k = 0, 1, ..., r-1, \qquad (27)$$

and note that $\sum_{k=0}^{r-1} y_k = 1$. Summing two of the equations in (26) with numbers $i = r-k-1$, $i = r+k$, we see that $y_0, ..., y_{r-1}$ must satisfy the system

$$ay_k + (2k+1)\sum_{j=0}^{k} y_j + \sum_{j=k+1}^{r-1} (2j+1)\, y_j = 2\lambda,\ k = 0, ..., r-1, \qquad (28)$$

which is equivalent to the system (26) under conditions (27). From (28) it follows that

$$ay_{r-1} + 2r - 1 = 2\lambda = 2P_{2r}(\mathbf{v}, a). \qquad (29)$$

and

$$a(y_{i+1} + y_{i-1}) = 2(a-1)y_i, \quad i = 0, 1, ..., r-2,$$

where we put $y_{-1} = y_0$. Thus if $y_0 \neq 0$, then the sequence

$$u_i = \frac{y_i}{y_0}, \quad i = 0, 1, ..., r-1$$

satisfies the recurrence

$$u_{i+1} = 2zu_i - u_{i-1}, \quad u_{-1} = 1, \quad u_1 = 1,$$

where $z = 1 - \frac{1}{a} = 1 - \frac{M}{n^2} = \cos\varphi$, and hence (see (24))

$$u_i = \frac{y_i}{y_0} = U_i(z) - U_{i-1}(z), \quad i = 0, 1, ..., r-1. \qquad (30)$$

Note that the condition $r\varphi < \pi/2 + \varphi/2$ implies (see (21)) that $u_i(z) = U_i(z) - U_{i-1}(z) > 0$ for all $i = 0, ..., r-1$. Since $U_{r-1}(z) = \sum_{i=0}^{r-1} u_i = 1/y_0 > 0$, (30) implies

$$y_i = \frac{U_i(z) - U_{i-1}(z)}{U_{r-1}(z)} > 0, \quad i = 0, 1, ..., r-1, \qquad (31)$$

and $\sum_{k=0}^{r-1} y_k = 1$. Thus, the coordinates of the point $v = (v_0, ..., v_{2r-1})$ defined by (27) and (31) satisfy the properties (17) and form a solution of the system (26). Together with (11), (16), and (29) this completes the proof. ■

Corollary 4: For any code $C \subseteq E^n$ of size M ($5 \leq M \leq n^2$),

$$\theta^2(C) \geq n - \left\lceil \frac{\pi n}{\sqrt{8M}} \right\rceil. \qquad (32)$$

Proof: There exists a unique integer r such that

$$r = \pi/(2\varphi) + \varepsilon$$

where $\cos\varphi = 1 - M/n^2$, $0 < \varphi \leq \pi/2$, and $-1/2 \leq \varepsilon < 1/2$. It is clear that $r \geq 1$ and $r\varphi < \pi/2 + \varphi/2$. Note that $\varphi > \sqrt{2M}/n$, because $2\sin^2\varphi/2 = M/n^2$. Therefore, for $M \geq 5$, $\pi/\varphi < \pi n/\sqrt{2M} < n$ and $\lceil \pi/\varphi \rceil \leq n$. Since $2r = \pi/\varphi + 2\varepsilon$ where $2\varepsilon < 1$, $2r \leq \lceil \pi/\varphi \rceil \leq n$. Thus, all conditions of Theorem 2 are satisfied for $5 \leq M \leq n^2$. In order to apply this theorem we need to estimate from above the value $\pi/(2\varphi) + g(\varepsilon)$ where

$$g(\varepsilon) = g(\varepsilon, \varphi) = \varepsilon + \frac{\cos\varepsilon\varphi - \cos(\varphi - \varepsilon\varphi)}{2(1 - \cos\varphi)\cos\varepsilon\varphi} - \frac{1}{2}.$$

It is easy to check that $g(-1/2) = g(0) = g(1/2) = 0$, $g(\varepsilon) \leq 0$ for $-1/2 \leq \varepsilon \leq 0$ and $g(\varepsilon) \leq \varepsilon$ for $0 \leq \varepsilon \leq 1/2$. This implies that $\pi/(2\varphi) + g(\varepsilon) \leq \lceil \pi/(2\varphi) \rceil$ for $-1/2 \leq \varepsilon < 1/2$, and completes the proof. ■

Since $2/\sqrt{3} = 1.1547$ and $\pi/\sqrt{8} = 1.1107$ the bound (32) is slightly better than (20). One can see that both bounds imply the asymptotic bound $\theta^2(C) \gtrsim n$ when the size M of codes $C \subseteq E^n$ tends to infinity as $n \to \infty$. In other words, we have proved that the lower asymptotic bound on minimum periodic crosscorrelation of binary codes [6], [8] is also valid for minimum aperiodic crosscorrelation. Note that at the same asymptotic process the Welch bound (14) yields only $\theta^2(C) \gtrsim n/2$.

IV. Concluding remarks and generalizations

In conclusion we note that these bounds can be improved when the size M of codes $C \subseteq E^n$ grows faster than a linear function of n, and this method can be extended to obtain new lower bounds on the aperiodic crosscorrelation of non-binary, real and complex codes. This is based on the consideration of other nonnegative definite functions on different spaces $W(\cdot)$. In particular, for the nonnegative definite functions $|\langle u, v\rangle|^{2k}$, $k = 1, 2, \ldots$, on $W(E^n)$ and any integer m, $1 \leq m \leq n$, our approach gives the following generalization of (19) for the minimum aperiodic crosscorrelation $\theta(n, M)$ of a code $C \subseteq E^n$ of size M:

$$\theta^{2k}(n, M) \geq \frac{M\left(\nu_k(n) + \frac{2}{m}\sum_{i=1}^{m-1} i\nu_k(n-m+i)\right) - n^{2k}}{Mm - 1}, \qquad (33)$$

where

$$\nu_k(n) = 2^{-n}\sum_{d=0}^{n} \binom{n}{d} (n-2d)^{2k}.$$

It is known [7] that $\nu_0(n) = 1$, $\nu_1(n) = n$, $\nu_2(n) = 3n^2 - 2n$, $\nu_3(n) = 15n^3 - 30n^2 + 16n$, and $\nu_k(n)$ is a polynomial of degree k in n. Moreover, one can show that $\nu_k(n)$ for $k \geq 1$ and $n \geq 2$ satisfies the following recurrence:

$$\nu_k(n) = -n(n-2)\nu_{k-1}(n)$$
$$+ n(n-1)\sum_{j=0}^{k-1} \binom{2k-2}{2j} 4^j \nu_{k-1-j}(n-2).$$

It follows by induction on k that the highest coefficient of $\nu_k(n)$ is equal to $(2k-1)!!$, where $(2k-1)!! = 1 \cdot 3 \cdots (2k-1)$. If k is fixed and $n \to \infty$, then considering in (33) $m = m(n)$ such that $m \to \infty$ and $m/n \to 0$ we get

$$\theta^{2k}(n, n^k) \gtrsim n^k (2k-1)!!. \qquad (34)$$

For comparison we note that the general form of the Welch bound [8]

$$\theta^{2k}(n, M) \geq \frac{M(2n-1)/\binom{2n-2+k}{k} - 1}{M(2n-1) - 1} n^{2k}$$

implies only that

$$\theta^{2k}(n, n^k) \gtrsim n^k k! 2^{-k}. \tag{35}$$

Denoting the ratio of the right-hand side of (34) to that of (35) by $\mu(k)$ we see that $\mu(k) = \binom{2k}{k}$ (in particular, $\mu(1) = 2$ as mentioned above) and that $\sqrt[2k]{\mu(k)} \to 2$ as $k \to \infty$.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Company, NewYork, 1968.

[2] A. Erdelyi, W. Magnus, F. Oberhettinger, and F.G. Tricomi, Higher Transcendental Functions, vol. 2, McGraw-Hill Book Company, NewYork, 1953.

[3] T. Helleseth and V. Kumar, "Sequences with low correlation", in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998.

[4] G. A. Kabatyanskii and V. I. Levenshtein, "Bounds for packings on a sphere and in space" (in Russian), *Problemy Peredachi Informatsii*, vol. 14, no. 1, pp. 3–25, 1978. English translation in *Probl. Inform. Trans.*, vol. 14, no. 1, pp. 1–17, 1978.

[5] V. I. Levenshtein, "Methods for obtaining bounds in metric problems of coding theory", in *Proc. of the 1975 IEEE-USSR Joint Workshop on Information Theory*, New York (1976), pp. 126–143.

[6] V. M. Sidelnikov, "On mutual correlation of sequences", *Dokl. Akad. Nauk SSSR*, vol. 196, no. 3, pp. 531–534, 1971. English translation in *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197–201, 1971.

[7] V. M. Sidelnikov, "On mutual correlation of sequences", in *Probl. Cybern.* 24, Nauka, Moscow, 1971, pp.15–42 (in Russian).

[8] L. R. Welch, "Lower bounds on the maximum cross-correlation of signals", *IEEE Trans. on Inform. Theory*, vol. 20, pp. 397–399, 1974.