Indian J. pure appl. Math., **39**(1): 69-86, February 2008

ON THE PAPR OF COSETS OF LINEAR CODES

PRABAL PAUL*, C. R. PRADEEP* AND B. SUNDAR RAJAN**

**Department of Mathematics, Indian Institute of Science, Bangalore* 12
e-mail: prabal@math.iisc.ernet.in; slearepi@gmail.com
***Department of E. C. E., Indian Institute of Science, Bangalore* 12
e-mail: bsrajan@ece.iisc.ernet.in

(*Received* 28 *August* 2006; *after final revision* 21 *August* 2007; *accepted* 13 *September* 2007)

Employing an error control code is one of the techniques to reduce the Peak-to-Average Power Ratio (PAPR) in a Orthogonal Frequency Division Multiplexing system, a well known class of such codes being the cosets of Reed-Muller codes. In this paper, we consider the class of such coset-codes of arbitrary linear codes and present a method of doubling the size of such a code without increasing the PAPR, by combining two such binary coset-codes. We identify the conditions under which we can employ this doubling more than once with no marginal increase in the PAPR value. Given a PAPR and length, our method has enabled to get the best coset-code (in terms of the size). Also, we show that the PAPR information of the coset-codes of the extended codes is obtainable from the PAPR of the corresponding coset-codes of the parent code. We have also shown a special type of lengthening is useful in PAPR studies.

Key Words: PAPR and affine linear codes

1. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) is a bandwidth efficient modulation scheme currently researched intensely and also part of several recent standards like IEEE 802.11 and 802.16. In spite of several advantages the OFDM systems enjoy, one of the main issues associated with these systems is the Peak-to-Average Power Ratio (PAPR) [1, 2]. One way of reducing the PAPR is to employ an error control code [3] which will essentially prevent sequences with high PAPR by way of not having them as codewords. It has been shown that certain cosets of Reed-Muller codes perform well for this purpose [1]. This paper studies cosets of arbitrary linear codes for the purpose of PAPR reduction.

Figure 1 shows a block diagram of a OFDM system with the encoder and the decoder blocks. The information bits to be communicated are mapped on to points of a complex signal constellation $\mathbb{Q}$ and the encoder encodes a set of k such complex symbols into a unique set of n constellation points of $\mathbb{Q}$ in every $\mathcal{T}$ seconds. This results in a Euclidean space code $\mathcal{C}$ of rate $R = k/n$. For every $\mathcal{T}$ seconds a codeword $\mathbf{c}$ of n constellation symbols are provided to the input of a discrete Fourier transform (DFT block) by a serial-to-parallel block, producing a sequence of n complex symbols $C_0, C_1, \ldots, C_{n-1}$ constituting the DFT vector of $\mathbf{c}$. This sequence is the input to the RF chain which produces the transmitted signal. This signal at time t is modeled by the real part of the complex envelope

$$S_{\mathbf{c}}(t) = \sum c_i e^{-\imath 2\pi (f_0 + i f_s)t} \quad (\imath = \sqrt{-1}) \tag{1.1}$$

for $0 \leq t \leq \dfrac{1}{f_s}$, where f_0 is the carrier frequency and f_s is the bandwidth of each tone. The relation between the quantities f_s and $\mathcal{T}$ depends on whether a guard time is assigned, or a cyclic prefix is used and these details have no bearing upon the bounds delivered in this paper. However, we note that $f_s = 1/\mathcal{T}$ is commonly assumed in an ideal situation. The receiver receives the signal $\Re(S_{\mathbf{c}}(t))$ perturbed by noise and performs the inverse operations.

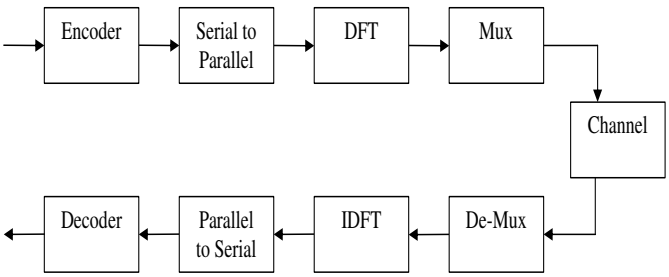

FIG. 1. Block diagram of an OFDM system

For any codeword $\mathbf{c}$, the instantaneous power of the corresponding transmitted signal $\Re(S_{\mathbf{c}}(t))$ is equal to $(\Re(S_{\mathbf{c}}(t)))^2$. This power is less than or equal to the function $|S_c(t)|^2$, called the *envelope power* of the OFDM signal. The average value of the envelope power is equal to $\|c\|^2$ while, for $f_0 \gg f_s$, the average power of the actual OFDM signal is approximately equal to $\dfrac{1}{2}\|c\|^2$. The PAPR associated with the OFDM signal corresponding to the codeword $\mathbf{c}$ denoted by $PAPR(c)$, is defined to be the ratio of the peak power of $\Re(S_{\mathbf{c}}(t))$ to $\|c\|^2$, the average envelope power. We

write $\zeta = f_0/f_s$, and note that in a typical OFDM application, we have $\zeta \gg 1$. Then we have

$$PAPR(\mathbf{c}) = \max_{0\le t\le 1} \frac{\left|\Re\Big(\sum_{i=0}^{n-1} c_i \exp(-2\pi\imath(\zeta+\mathrm{i})\mathrm{t})\Big)\right|^2}{\|c\|^2}. \tag{1.2}$$

Note that

$$PAPR(\mathbf{c}) \le \max_{0\le t\le 1} \frac{|S_c(t)|^2}{\|c\|^2}.$$

The expression on the right of the above inequality is called the peak-to-mean envelope power ratio (PMEPR) of the codeword or the corresponding OFDM signal. We denote it by $PMEPR(c)$. It is often more convenient to work with PMEPR than PAPR. It is straightforward to show that if

$$c(z) = c_0 + c_1 z + ... + c_{n-1} z^{n-1} \tag{1.3}$$

denotes the degree $n-1$ polynomial whose coefficients are derived from $\mathbf{c}$, then

$$PMEPR(\mathbf{c}) = \frac{1}{\|c\|^2} \max_{|z|=1} |c(z)|^2.$$

The PMEPR of a codeword is related to the maximum squared absolute value of the corresponding polynomial on the unit circle. This observation will be useful in the sequel.

For a code $\mathcal{C}$,

$$PAPR(\mathcal{C}) = \max_{\mathrm{c}\in\mathcal{C}}(\mathcal{PAPR}(\mathcal{C}))$$

is called the peak-to-average power ratio of the code denoted by $PAPR(\mathcal{C})$.

The contributions of this paper are listed below:

- We provide a method of combining two coset-codes of a binary linear code which leads to another coset-code of some other code with double the size but no increase in the PMEPR. We identify the conditions under which this is possible along with conditions under which this doubling the size can be employed more than once.
- We study the PAPR properties of coset-codes of the extended codes (obtained by adding the parity check symbol at the beginning or end of all the codewords) in terms of the PAPR of the coset-codes of the parent code which can be over finite fields $\mathbb{F}_q$ or over integer residue class rings $\mathbb{Z}_m$. As a consequence of this we show existence of codes of large length with PAPR as close to 2 as desired.

The remaining part of the content is organized as follows: In Section 2 we obtain our method of combining cosets, called Cosets-Combining, by identifying the relevant mathematical results. We illustrate our method with several examples which lead to different possible situations when

the Cosets-Combining is employed. Section 3 presents the PMEPR properties of coset-codes of extended codes (both at the beginning and at the end of the codewords) in terms of the PMEPR of the coset-codes of the parent codes. In section 4 we have defined and shown the usefulness of a special type of lengthening and we have able to obtain new coset-code of squaring size and doubling length and doubling PMEPR from the original coset-code.

2. The Method of Cosets-Combining

In this section we are primarily concerned with binary error control codes used in conjunction with binary antipodal constellation, except in the last subsection where we briefly discuss the issues concerned with non-binary codes. From the definition of PMEPR, it is clear that the linear codes are not suitable for use since the all zero codeword will give the highest PAPR. But an arbitrary nonlinear code has the problem of specifying the code itself along with the problem of decoding. This motivates the study of cosets of linear codes as codes for PAPR reduction, which are essentially non-linear codes but have structure as well and do not contain codewords that lead to the highest values of PAPR. We call the cosets of a linear code $\mathbf{C}$ as *coset-codes* of $\mathbf{C}$.

In this section, we address the problem of constructing coset-codes of large size with small PMEPR. We give a method which under appropriate conditions results in doubling of the code size with no increase in the PMEPR. We call this the method of Coset-Combining. We explain this in the following subsection and illustrate this with several examples and justify our claims with explicit computations in the subsequent subsection.

2.1 Cosets-Combining

Our method of Cosets-Combining exploits the following result:

***Theorem* 1** — *Suppose S is an r-dimensional subspace of an n-dimensional vector space over $\mathbb{F}_2$. If Q and R denote two cosets of S. Then there exists a vector subspace T containing S such that the union of Q and R is a coset of T.*

Proof: The following three cases exhaust the possibilities for Q, S and R.

Case 1: $Q = R$

In this case, $T = S$.

Case 2: $Q \neq R$, but $S = Q$ or $S = R$.

Without loss of generality, we may assume that $S = Q$. Clearly, in this case, r is strictly less than n. Take any $\alpha \in R$, and let T be the subspace generated by S and α. Then α does not belong to S. So, Cardinality of T is twice the cardinality of S which is same as the Cardinality of $(Q \sqcup R)$. Now, $\beta \in S$ implies $\beta \in T$. For $\gamma \in R$ implies $\gamma + \alpha \in S$ (as both $\alpha, \gamma \in R$) and hence $\gamma + \alpha \in T$, but, $\alpha \in T$, therefore $\gamma = \gamma + \alpha + \alpha \in T$. Hence, $Q \sqcup R \subseteq T$. As the cardinalities of T and $Q \sqcup R$ are same and finite, we have $Q \sqcup R = T$.

Case 3: $Q \neq R$ and $Q \neq S \neq R$.

In this case, take any $\alpha \in Q$ and $\beta \in R$. Let, $\gamma = \alpha + \beta$. Let T be the subspace generated by S and γ. Clearly, γ does not belong to S (as otherwise, $\beta = \alpha + \beta + \alpha = \gamma + \alpha \in Q$, so $Q \cap R \neq \phi$ and hence $Q = R$, a contradiction to the assumption). Let C be the coset of T containing α. Then $\beta = \alpha + \beta + \alpha = \gamma + \alpha \in C$. Now let us take any $\delta \in Q$. Therefore, $\delta + \alpha \in S \subseteq T$. Hence, $\delta = \alpha + (\delta + \alpha) \in C$. Therefore, $Q \subset C$. Similarly, it can be shown that $R \subset C$. Hence, $Q \cup R \subseteq C$. But, as cardinality of $Q \cup R$ is same as the cardinality of C (which is finite), therefore $C = Q \cup R$.

Cosets-Combining — Let S be a k-dimensional subspace of $\mathbb{F}_2^n$. Let $S_1, S_2, \ldots, S_t$ be the cosets of S where $t = 2^{n-k}$, with the PMEPR values, respectively, P_1, P_2, ..., P_t. Without loss of generality, let $P_i \leq P_j$ for $i = 1, 2$ and for all $j = 3, 4, ..., t$. Then from Proposition 1, there exists a subspace $T(\supset S)$ such that $S_1 \cup S_2$ is a coset of T and clearly the PMEPR of $S_1 \cup S_2$ is $\max\{P_1, P_2\}$. Moreover, this coset will have the least PMEPR among all the cosets of T with the increase in PMEPR being $P_2 - P_1$. Notice that if $P_1 = P_2$ then the size can be doubled without increase in the PMEPR. This method of taking union of two cosets of a linear code with the smallest values of PMEPR and viewing as a coset code of another code is called **Cosets-Combining**. The code S will be referred as the original code, and the notation S' will be used to indicate the code T.

The following corollary shows that the best binary affine-linear codes with a given $PAPR$ can be obtained using our Coset-Combining method (starting from the trivial subspace) and given a binary linear code and a given $PAPR$, it is possible to construct the best super-space which has a coset of $PAPR$ less than or equals to the given $PAPR$. In fact, given a fixed length and a fixed $PAPR$, one can get all possible affine linear codes of that length whose $PAPR$ is not greater than the given $PAPR$.

Corollary 2 — (Construction theorem). Any binary linear code having a coset with low PMEPR can be obtained using our Cosets-Combining method iteratively starting from the trivial sub-space.

PROOF: Let L be a binary linear $[n, k]$ code generated by $\{u_1, u_2, \cdots, u_k\}$ where $u_i = (u_{i1}, u_{i2}, \cdots, u_{in})$ $\forall\ i = 1, 2, \cdots, k$. Let C be a coset of L having smallest $PMEPR$ among all the cosets of L. Let $c = (c_1, c_2, \cdots, c_n)$ be a coset representative of C. Let, p be the $PMEPR$ of C. Now, this corollary will be proved using mathematical induction on the number of iteration.

Firstly, note that $c,\ u_1 + c \in C$. Therefore, $PMEPR(c),\ PMEPR(u_1 + c) \leq p$. Hence by applying our coset-combining method, we will get a vector space L_1 (say) generated by $c + (u_1 + c) = u_1$ such that it has a coset $C_1 = \{c\} \sqcup \{u_1 + c\}$ whose $PMEPR$ is not greater than p.

Now suppose L_i have been defined for $i < k$ where L_i is generated by $\{u_1, u_2, \cdots, u_i\}$. Let, C_i be the coset of L_i having c as the coset representative. Now, let C_i' be the coset of L_i having $c + u_{i+1}$ as the coset representative. Now, it is clear that $C_i \subseteq C$ and $C_i' \subseteq C$. Therefore, $PMEPR(C_i),\ PMEPR(C_i') \leq p$. Note that C_i and C_i' are two distinct cosets of L_i. Hence,

by applying our coset-combining method, one can get a binary vector subspace of dimension $i+1$ generated by L_i and $c+(c+u_{i+1})=u_{i+1}$ i.e, generated by $\{u_1,u_2,\cdots,u_{i+1}\}$ such that it has a coset $C_i \sqcup C_i'$ whose $PMEPR$ is less than or equals to p and c is a coset representative for $C_i \sqcup C_i'$.

Hence, by using mathematical induction, we obtain the binary linear code L after k iterations using coset-combining method.

This completes the proof.

Definition 1 — For a vector $c=(c_0,c_1,\ldots,c_{n-1})\in\mathbb{F}_q^n$, we define $PR'(c)$ as $PR'(c)=\max_{|z|=1}|c(z)|$, where $c(z)=\sum_{0\leq i\leq n-1}\omega^{f(c_i)}z^i$ (ω is a primitive q th root of unity in the field of complex numbers and $f:\mathbb{F}_q\to\mathbb{Z}_q$ is any fixed bijective map). For a code $C\subseteq\mathbb{F}_q^n$, we define, $PR'(C)=\max_{c\in C}PR'(c)$. For codes over $\mathbb{Z}_m$ this definition applies with the map f being the identity map.

It is clear from the above definitions that $PMEPR(c)=\frac{1}{n}PR'(c)^2$ and $PMEPR(C)=\frac{1}{n}PR'(C)^2$.

Proposition 3 — Let L be a sub-module of $\mathbb{Z}_m^n$ over $\mathbb{Z}_m$ such that $(1,1,\cdots,1)$ does not belongs to L. Let C be a coset of L and let $c=(c_1,c_2,\cdots,c_n)$ be a coset-representative of C. Let, C' be the coset of L whose coset representative is $c'=(c_1+1,c_2+1,\cdots,c_n+1)$. Then the $PMEPR$ of C and C' are same and hence the number of cosets of L having a given $PMEPR$ is a multiple of m.

PROOF: It is clear that $C\neq C'$. Let $\omega=e^{\frac{2\pi\imath}{m}}$ be a primitive mth root of unity. Now, it is also clear that $C'=C+(1,1,\cdots,1)$. Now, let us take any $d=(d_1,d_2,\cdots,d_n)\in C$. Then, $d'=(d_1+1,d_2+1,\cdots,d_n+1)\in C'$. Now,

$$\begin{aligned}
PR'(d') &= \max_{|z|=1}|\omega^{d_1+1}+\omega^{d_2+1}z+\cdots+\omega^{d_n+1}z^{n-1}|\\
&= \max_{|z|=1}|\omega[\omega^{d_1}+\omega^{d_2}z+\cdots+\omega^{d_n}z^{n-1}]|\\
&= \max_{|z|=1}|\omega^{d_1}+\omega^{d_2}z+\cdots+\omega^{d_n}z^{n-1}|\\
&= PR'(d)
\end{aligned}$$

and hence $PMEPR(d)=PMEPR(d')$ and hence, $PMEPR(C)=PMEPR(C')$. This completes the proof.

Now, consider the following easy and useful corollary:

Corollary 4 — Let M be a sub-module of $\mathbb{Z}_m^n$ over $\mathbb{Z}_m$ such that $(1,1,\cdots,1)$ does not belongs to M. Let $C=C^{(0)}$ be a coset of M. Let $c=(c_1,c_2,\cdots,c_n)$ be a coset-representative of C. Let $C^{(i)}$ be the coset of M whose coset representative is $(c_1+i,c_2+i,\cdots,c_n+i)$, $\forall i=1,2,\cdots,m-1$. Let M_1 be the sub-module generated by M and $(1,1,\cdots,1)$. Then, $\cup_{i=0}^{m-1}C^{(i)}$ is a coset of M_1.

The importance of the above proposition and the corollary lie in the fact that if $M(\subseteq\mathbb{Z}_m^n)$ is a sub-module such that $(1,1,\cdots,1)$ does not belongs to M and if M_1 is the sub-module of $\mathbb{Z}_m^n$

generated by M and $(1, 1, \cdots, 1)$, then the minimum $PMEPR$ of all cosets of M and M' are same i.e. we can increase the size m times by keeping the $PMEPR$ fixed.

In the following subsection we illustrate Cosets-Combining with several known codes and sometimes with repeated applications of it. The resulting coset codes and the values of PMEPR are also given. To make the job of computing the PMEPR computationally less intensive the following two propositions are useful of which the first proposition is easy and straightforward.

Proposition 5 — For any binary vector $b = (b_0, b_1, ..., b_{n-1}) \in \{0, 1\}^n$,

$$PMEPR(b) = \frac{1}{\|c\|^2} \max_{0 \le \theta \le \pi} |c(e^{i\theta})|^2,$$

where $c(z) = c_0 + c_1 z + c_2 z^2 + ... + c_{n-1} z^{n-1}$, $c_i = (-1)^{b_i}$ for $i = 0, 1, ..., (n-1)$, $c = (c_0, c_1, ..., c_{n-1})$, and $\|.\|$ denotes the Euclidean norm.

Proposition 6 — Let K be a $(k+1)$ dimensional vector subspace of the n_1 dimensional vector space over $GF(2)$ and B an k dimensional vector subspace of K. Let $D_1, \ldots, D_{2r}$ be the list of all cosets of B and d_i is the coset representative of the coset D_i for all $i = 1, \ldots, 2r$. Then $D_m \sqcup D_n$ is a coset of K iff $d_m + d_n \in K$ $(m \neq n)$.

PROOF: Firstly, suppose $D_m \sqcup D_n$ is a coset of K, then $d'_m + d'_n \in K$ for all $d'_m \in D_m$ and $d'_n \in D_n$. So, in particular, $d_m + d_n \in K$. Conversely, since $B \subset K$, we have $d_m + B \subset d_m + K$ and $d_n + B \subset d_n + K$, that is, $D_m \subset d_m + K$, $D_n \subset d_n + K$. But, $d_m + K = d_n + K$ as $d_m + d_n \in K$. Therefore $D_m \sqcup D_n \subset d_m + K$. Their cardinalities being equal, we have $D_m \sqcup D_n = d_m + K$.

Notice that the importance of the Proposition 6 lies in the fact that it determines which two of the cosets should be joined while applying the Cosets-Combining method.

In all the examples discussed in this paper, we have computed PMEPRs using Matlab by partitioning the interval $[0, \pi]$ into 100 parts.

2.2. EXAMPLES

In this subsection, we illustrate the method of Cosets-Combining for several standard binary linear codes explicitly. Table 1 summarizes the relevant features of the examples of this subsection. The code $\mathcal{C}_3$ in the following example seems to be one with the lowest PMEPR for its length. However, the Cosets-Combining technique can not be directly applied to non-binary codes since the Theorem 1 is true only for binary codes.

Example 1 :

1. Let $\mathcal{C}_1$ denote the simplex code whose generator matrix is

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

   It has 16 cosets out of which there are 2 cosets for each of the PR' values 7, 5.0975, and 5.0636 and for the rest of the ten cosets the PR' is 5. By repeating our Cosets-Combining three times, we could increase the size of the code 8 times without increasing the PMEPR. The details are given in the first row of Table 1.

2. Let $\mathcal{C}_2$ denote the length 15 simplex code whose generator matrix is

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

   It has 2048 cosets out of which the smallest PMEPR ones are only two. So, we can carry out our Cosets-Combining only once if we do not permit any increase in the PMEPR. However, we could apply thrice with marginal increase in the PMEPR. The second row of the Table 1 shows the details.

3. Let $\mathcal{C}_3$ be the Reed-Muller code $RM_2(1,3)$ which is a subspace of $\mathbb{F}_2^8$. It has 3 cosets with the smallest PMEPR which is 2 out of the total of 16 cosets. We apply our Cosets-Combining only once to double the size without increase in PMEPR as shown in the third of Table 1.

4. Let $\mathcal{C}_4$ be the Reed-Muller code $RM_2(1,4)$ which is a subspace of $\mathbb{F}_2^{16}$. Out of the total of 2048 cosets of this code the number of cosets with the smallest PMEPR was computed to be only one. So, we can not use our Cosets-Combining with out increase in PMEPR. However, 12 cosets were seen to be with PMEPR less than or equal to 2. So, we applied our Cosets-Combining with the criterion of keeping the PMEPR less than or equal to 2. For this objective we could increase the size of the code four times by applying our method twice as shown in the fourth row of Table 1.

5. Let $\mathcal{C}_5$ be the length 7 BCH code with the generator polynomial $1 + x + x^3$. The dimension of $\mathcal{C}_5$ is 4 and it has 8 cosets among which 2 cosets are with PMEPR 3.5714, 4 cosets are with PMEPR 3.7121 and the remaining 2 are with PMEPR 7. In this case by using our method twice, we could increase the size 4 times and get a coset-code with PMEPR 3.7121. The fifth row of Table 1 shows the remaining details.

6. Our next code is a Quadratic Residue code. It is known that 2 is a quadratic residue mod a prime p iff p is of the form $8k+1$ or $8k+7$ ($k \geq 0$). We start with the prime $17 = 8.2+1$. The factorization of $x^{17}+1$ over F_2 is $x^{17}+1 = (1+x)(1+x+x^2+x^4+x^6+x^7+x^8)(1+x^3+x^4+x^5+x^8)$. We take $(1+x+x^2+x^4+x^6+x^7+x^8)$ as the generator polynomial of the quadratic residue code. It is a cyclic code $\mathcal{C}_6$ (say) of length 17 and size 2^9. Out of the total of 256 cosets of this code four of them have the minimum PMEPR of value 7.1176. Hence, by applying our method twice, we get an affine linear code of size 2^{11} with PMEPR 7.1176 as shown in the sixth row of Table 1.

7. Let $\mathcal{C}_7$ be the code obtained by puncturing the first coordinate of the code $\mathcal{C}_6$. The size of $\mathcal{C}_7$ is 2^9. It has only two cosets of the smallest value for PMEPR equal to 7.6417. By employing Cosets-combining once, we have been able to double the size by keeping the PMEPR fixed. Table 1 gives further details. It is interesting to note that puncturing has increased the PMEPR. We do not know whether it is true in general.

8. Let $\mathcal{C}_8$ be the extended code of $\mathcal{C}_1$ obtained by adding a even parity at the end of the codeword. This length-8 code has two cosets with PMEPR 3.2954 (which is the minimum of the PMEPRs all the cosets). Hence, by applying our method, we get a coset-code of length 8 and size 16 with PMEPR 3.2954. If we implement our method again, we get a code of size 32 but the PMEPR increases to 3.3465.

9. We consider the extension of $\mathcal{C}_2$ with respect to the last co-ordinate. The size as well as the length of the resulting code $\mathcal{C}_9$ is 16 and has 4096 cosets. There are 2 cosets with PMEPR 2.9348 (which is the minimum). Hence, by applying our method once we get a coset-code of size 32 with no increase in PMEPR.

3. Coset-Codes of Extended Codes

For a given n-length code $\mathcal{C}$ over a field or a ring, if to every codeword $(c_0, c_1, \cdots, c_{n-1})$ the check sum $c_n = (c_0 + c_1 + \cdots + c_{n-1})$ is added at the end to get $(c_0, c_1, \cdots, c_{n-1}, c_n)$ the resulting code is called the right-extended code and if it is added at the beginning to get $(c_n, c_0, c_1, \cdots, c_{n-1})$, the resulting code is called the left-extended code. In this section, we study the PMEPR properties of the the coset codes of the extended codes over finite fields (both binary and non-binary) [4] and over the ring $\mathbb{Z}_m$ of integers modulo m.

The following straightforward lemma is useful.

Lemma 7 — Let c' be the right-extended vector of the vector $c = (c_0, c_1, \cdots, c_{n-1}) \in F_q^n$. Then $PR'(c') \leq PR'(c) + 1$.

A straightforward consequence of Lemma 7 is

Table 1: Numerical data of the above nine examples

Code $\mathcal{C}$	n	$\|\mathcal{C}\|$	M_1	M_2	d	N	G_{add}	M_1'	d'
$\mathcal{C}_1$	7	8	3.5714	3.5714	(1,1,-1,1,1,1,1)	3	(-1,-1,-1,-1,-1,-1,-1) (1,1,1,-1,1,1,1) (1,1,1,1,1,-1,1)	3.5714	(1,1,1,1,-1,1,1)
$\mathcal{C}_2$	15	16	2.6781	2.6781	(1,1,1,1,-1,1,1,1, -1,-1,-1,1,-1,1,1)	3	(1,1,-1,-1,1,1,-1,1 -1,-1,1,1,-1,-1,1) (1,1,1,1,1,-1,-1,1, -1,1,-1,1,-1,-1,1) (1,1,1,1,1,1,-1,-1, -1,-1,1,-1,1,1,1)	2.8528	(1,1,1,1,-1,1,1,1, -1,-1,-1,1,-1,1,1)
$\mathcal{C}_3$	8	16	2	2	(-1,1,1,-1,1,1,1,1)	1	(-1,-1,-1,1,1,-1,1,1)	2	(-1,1,1,-1,1,1,1,1)
$\mathcal{C}_4$	16	32	1.9664	1.9956	(1,1,1,-1,1,1,-1,1 1,1,1,-1,-1,-1,1,-1)	2	(-1,1,1,1,1,1,1,-1 -1,-1,-1,1,-1,1,1,1), (1,1,1,1,1,1,-1,-1 1,1,-1,-1,1,1,1,1)	≤ 2	(-1,1,1,-1,1,1,1,1 -1,-1,1,1,1,-1,1,-1)
$\mathcal{C}_5$	7	16	3.5714	3.5714	(1,1,1,1,1,1,-1)	2	(1,1,1,1,-1,1,1) (1,1,1,1,1,-1,1)	3.7121	(1,1,1,1,1,1,-1)
$\mathcal{C}_6$	17	2^9	7.1176	7.1176	(1,1,1,1,1,1,1,1,1, 1,1,-1,-1,-1,1,1,1)	2	(1,1,1,1,1,1,1,1, 1,-1,1,-1,-1,1,1,-1,1) (1,1,1,1,1,1,1,1,1, -1,1,-1,1,1,1,1,-1)	7.1176	(1,1,1,1,1,1,1,1,1, 1,1,-1,-1,-1,1,1,1)
$\mathcal{C}_7$	16	2^9	7.6417	7.6417	(1,1,1,1,1,1,1,1, 1,1,1,-1,-1,1,-1,1)	1	(1,1,1,1,1,1,1,1, 1,-1,1,-1,-1,1,1,-1)	7.6417	(1,1,1,1,1,1,1,1, 1,1,1,-1,-1,1,-1,1)
$\mathcal{C}_8$	8	8	3.2954	3.2954	(1,1,-1,1,1,-1,1,1)	2	(1,1,-1,1,-1,-1,1,-1) (1,1,1,-1,1,-1,1,1)	3.3465	(1,1,-1,1,1,-1,1,1)
$\mathcal{C}_9$	16	16	2.9348	2.9348	(1,1,1,1,-1,1,1,1 1,-1,1,-1,-1,-1,1,1)	1	(1,1,-1,-1,1,1,-1,1, -1,-1,1,1,-1,-1,1,-1)	2.9348	(1,1,1,1,-1,1,1,1 1,-1,1,-1,-1,-1,1,1)

NC= Number of cosets, n= Length of the code , $|\mathcal{C}|$=Size, M_1 = Minimum PMEPR among all the cosets of $\mathcal{C}$, M_2 = 2nd minimum PMEPR among all the cosets of $\mathcal{C}$, d = A coset representative for the coset with minimum PMEPR of the original code, N = Number of times we are applying our method, G_{add} = Additional vectors in the generator matrix of $\mathcal{C}$, M_1' = Minimum PMEPR among all the cosets of the new code obtained by applying our method N times, d' = A coset representative for the coset with minimum PMEPR of the new code.

***Theorem* 8** — *Let L be a linear $[n,k]$ code over $\mathbb{F}_q$ and let E be the right-extended code of L. Let $c = (c_0, c_1, \cdots, c_{n-1}) \in L$ with the corresponding $c' = (c_0, c_1, \cdots, c_n) \in E$. Let $\mathbf{C}$ be*

the coset of L in $\mathbb{F}_q^n$ whose coset representative is c and $\mathbf{C}'$ be the coset of E in $\mathbb{F}_q^{n+1}$ whose coset representative is c'. Then, $PR'(\mathbf{C}') \leq PR'(\mathbf{C}) + 1$. This is true if L is over $\mathbb{Z}_m$ instead of over $\mathbb{F}_q$.

Corollary **9** — The L be a linear code over $\mathbb{F}_q$ and λ be the minimum PR' of all cosets of L. Let E be the right-extended code of L. Then the minimum of PR' of all the cosets of E is less than or equal to $\lambda + 1$. This is true if L is over $\mathbb{Z}_m$ instead of over $\mathbb{F}_q$.

The following is an interesting theorem.

***Theorem* 10** — *For any given real number $\epsilon > 0$, there exists a positive integer $N(\epsilon)$ such that for every $k \geq N$ there exists a binary code of length $2^k + 1$ with PMEPR less than or equal to $2 + \epsilon$.*

PROOF: Since for every $n = 2^k$ (where k is a natural number), there exists a binary affine linear code of PMEPR at most 2 (see [1] for reference), let us take an n which is of the form 2^k and a linear code L_n such that it has a coset C_n (say) with PMEPR at most 2. Hence PR' of C_n is at most $\sqrt{2n}$. Let, E_n be the extension of L_n with respect to the last co-ordinate. Therefore, by the previous theorem, E_n has a coset E'_n (say) such that the PR' of E'_n is at most $\sqrt{2n} + 1$. Therefore, $PMEPR(E'_n) \leq \frac{PR'(E'_n)}{n+1} \leq \frac{(\sqrt{2n}+1)^2}{n+1} = \frac{2n+2\sqrt{2n}+1}{n+1} = 2\frac{n}{n+1} + \frac{2\sqrt{2n}}{n+1} + \frac{1}{n+1} \longrightarrow 2$ as $k \longrightarrow \infty$.

Hence by the basic definition of limit, we can easily see that the above theorem is true.

Corollary 11 — The above theorem holds for linear codes over $\mathbb{Z}_{2^r}$ for any $r > 1$ also.

In a similar way the following can also be established:

Corollary 12 — For any given real number $\epsilon > 0$ and a positive integer r there exists a positive integer $N(\epsilon, r)$ such that for every $k \geq N$ there exists a code of length $2^k + r$ with PMEPR less than or equal to $2 + \epsilon$.

For a given binary linear code L, let $P_1 \leq P_2 \leq P_3 \leq \ldots \leq P_t$ be the PMEPR of all the t cosets of L and let $p_1 \leq p_2 \leq \ldots \leq p_t$ be the PR' of the respective cosets and let C_i be the coset whose PMEPR is P_i for all $i = 1, \ldots, t$. Also let $c_i = (c_{i1}, c_{i2}, \ldots, c_{in})$ be the coset representative of the coset C_i for all $i = 1, 2, \ldots, t$. Let, E be the right-extended code of L, and C'_i be the coset of E whose coset representative is $(c_{i1}, c_{i2}, \ldots, c_{in}, 0)$ and C''_i be the coset of E whose coset representative is $(c_{i1}, c_{i2}, \ldots, c_{in}, 1)$ for all $i = 1, 2, \ldots, t$. Let, P'_i and p'_i respectively be the PMEPR and PR' of the coset C'_i and also let, P''_i and p''_i respectively be the PMEPR and PR' of the coset C''_i for all $i = 1, \ldots, t$. It is clear that, $C'_i \neq C'_j$ and $C''_i \neq C''_j$ for $i \neq j$ and also, $C'_i \neq C''_j$ for all $i, j = 1, \ldots, t$. The $2t$ cosets of E are precisely C'_i and C''_i for all $i = 1, \ldots, t$. Now, for a given $1 \leq l \leq t$, we can have at least $2l$ number of cosets of E whose PR' are less than or equal to $p'_l + 1$, i.e. we are increasing the dimension of the affine linear code after extension and in that case we are increasing PR' by one only. Therefore, in the extension method, we can easily see that we can implement our joining coset method more number of times without substantial increase in PR'.

Proposition 13 — Let L be a subspace of $\mathbb{Z}_m^n$ and E be the right-extended code of L. Let λ be the minimum of PR' of all cosets of L. Let E_1 be the subspace of $\mathbb{Z}_m^{n+1}$ generated by E and $(0,0,\ldots,0,1) \in \mathbb{Z}_m^{n+1}$. Then the minimum of PR' all the cosets of E_1 is less than or equal to $\lambda+1$. Moreover if $c=(c_1,\ldots,c_n)$ is the coset representative of the cosets of L having minimum PR', then the coset of E_1 having $(c_1,\cdots,c_n,1)$ as a coset representative has PR' less than or equal to $\lambda+1$.

PROOF: Let L be a sub-module of $\mathbb{Z}_m^n$. Let E be the extension of L with respect to the last co-ordinate. Let, C be the coset of L having smallest $PMEPR$ among all the cosets of L. Let, $c=(c_1,\ldots,c_n)$ be a coset representative of C. Let, E_1 be the sub-module of $\mathbb{Z}_m^{n+1}$ generated by E and $(0,0,\ldots,0,1)(\in \mathbb{Z}_m^{n+1})$. Now, let C_1 be the coset of E_1 having $(c_1,\ldots,c_n,1)$ as coset representative. Now, let us take any $(d_1,d_2,\ldots,d_n) \in C$. Then, $(d_1-c_1,d_2-c_2,\ldots,d_n-c_n) \in L$ and therefore, $(d_1-c_1,d_2-c_2,\ldots,d_n-c_n,\sum c_i-\sum d_i) \in E \subset E_1$. Let, $\alpha=\sum c_i-\sum d_i+1 \pmod m$. Then, $(d_1-c_1,d_2-c_2,\ldots,d_n-c_n,\sum c_i-\sum d_i)+(c_1,c_2,\ldots,c_n,1)=(d_1,d_2,\ldots,d_n,\alpha) \in C_1$ and hence$(d_1,d_2,\ldots,d_n,\alpha+1) \in C_1$ as $(0,0,\ldots,0,1) \in E_1$. Therefore, $C_2=\{(d_1,d_2,\ldots,d_n,k)/(d_1,d_2,\ldots,d_n) \in C, k=0,1,\ldots,m-1\} \subseteq C_1$. It is clear that Cardinality of C_2= (Cardinality of L) $\times m$ and Cardinality of L= Cardinality of E. But, Cardinality of $E_1 \leq$ (Cardinality of E) $\times m$. Therefore, Cardinality of C_2= Cardinality of C_1= Cardinality of E_1 (which is finite). Therefore, $C_1=C_2$. Now it is clear that $PR'(C_1) \leq PR'(C)+1$.

Corollary 14 — Let L be a sub module of $\mathbb{Z}_m^n$ and E be the right-extended code of L. Also, let E_1 be the sub module of $\mathbb{Z}_m^{n+1}$ generated by E and $(0,0,\ldots,0,1)(\in \mathbb{Z}_m^{n+1})$. Now, if L has l cosets of PR' less than or equal to λ, then E_1 has at least l cosets of PR' less than or equal to $\lambda+1$.

PROOF: It is clear from the above proposition that if $(c_1,\ldots,c_n)(\in \mathbb{Z}_m^n)$ is the coset representative of the coset C (say), and if PR' of C is less than or equal to pr', then the PR' of the coset of E_1 having $(c_1,\ldots,c_n,1)$ as coset representative is less than or equals to $pr'+1$. Hence, in order to complete the proof we only need to show that different cosets of L correspond to the different cosets of E_1. Let, $(c_1,\ldots,c_n)$ and $(d_1,d_2,\ldots,d_n)$ are different coset representatives of L. Let, C and D respectively be the cosets of L having $(c_1,\ldots,c_n)$ and $(d_1,d_2,\ldots,d_n)$ as coset representatives. Then by the above proposition, $C \times \mathbb{Z}_m$ and $D \times \mathbb{Z}_m$ are the corresponding cosets of E_1 and clearly they are disjoint.

The following corollary is very useful to have a reasonably good Hamming distance while extending a code and increasing the size of the code. The first part of the following corollary is immediate from Corollary 12 and Proposition 13.

Corollary 15 — For any given real number $\epsilon > 0$ and a positive integer r there exists a positive integer N (depending on ϵ, r) such that for every $k \geq N$ there exists a $[2^k+r, 1+\binom{k}{1}+r]$ binary linear code which has a coset with PMEPR less than or equals to $2+\epsilon$. Moreover, for any $0<d\leq r$, there is a $[2^k+r, 1+\binom{k}{1}+k_1, d_1]$ binary linear code which has a coset with PMEPR less than or

equals to $2+\epsilon$ (where k_1 is the maximum of all subspaces of $\mathbb{Z}_2^r$ whose minimum Hamming distance is at least d and $d_1 = \min(d, 2^{k-1})$).

It can be shown that Proposition 13 and Corollary 14 holds for linear codes over finite fields F_q. In the following subsection we construct several such codes using this Proposition.

All the results stated in this section so far for right-extended codes in the form of Lemma, Theorems, Corollaries and Propositions hold for left-extended codes also.

3.1 EXAMPLES

In this subsection we compute the PMEPR of all coset-codes of several extended linear codes (over finite fields and finite rings) constructed using Proposition 13. We consider both the left and the right extended codes to show that the resulting PMEPRs can be different even though the bound for them is the same.

Example 2 — (Continuation of Example 1)

1. After applying Cosets-Combining thrice on the code $\mathcal{C}_1$ of Example 1 the resulting code is left-extended. Applying Cosets-Combining on this left-extended code gives a binary linear code of length 8, size 128 and it has a coset of PR' 6 i.e PMEPR 4.5. In this case right-extending the code leads to the same situation.

2. Applying Cosets-Combining once on the left-extended code of $\mathcal{C}_2'$ of Example 1 gets a binary linear code of length 16 and size 256 such that it has a of PR' 7.5247 ($\leq$7.5415) i.e. of PMEPR 3.5388. However, applying Cosets-Combining on the right-extended code gets a binary linear code of same size but with a different PR' which is 7.5391 (($\leq$7.5415) i.e. of PMEPR 3.5524.

3. The code $\mathcal{C}_3$ of Example 1 after undergoing Cosets-Combining get left-extended. This new code has 2 cosets with PR' equals to 5. By applying our Cosets-Combining method again, we get a binary linear code of length 9, size 64 having a coset of PR' 5 i.e, PMEPR $\frac{25}{9} = 2.7778$. Right-extending the code does not give a different result.

4. The code $\mathcal{C}_4'$ of Example 1 has a coset with PR' less than or equal to $5.6569 = \sqrt{32}$. The left-extended code is this code has two cosets with PR' 6.6527. Now, by Cosets-Combining once more we get a coset-code of length 17 and size 256 with PR' is 6.6527 i.e. PMEPR 2.6034. In this case right-extending the code results in the same set of numbers.

5. For the code $\mathcal{C}_5$ of Example 1, we have seen that after applying our Cosets-Combining method twice, we got a new binary linear coset-code with PMEPR 3.7121. Now, if we left-extend the new code obtained after combining twice and apply our Cosets-Combining we get a new

binary linear code of length 8 and size 128 with PMEPR 4.5. If we see the right-extended code, the resulting PMEPR remains same.

We end this section with the following example of codes over $\mathbb{Z}_4$.

Example 3 — Let us consider a submodule M generated by $\{(0,1,0,1,0,1,0,1), (0,0,1,1,0,0,1,1), (0,0,0,0,1,1,1,1), (1,1,1,1,1,1,1,1)\}$ over $\mathbb{Z}_4$. The minimum PR' of all the cosets of M turns out to be 4 and there are three cosets with this value of PR'. Now, we left-extend the code M and then introduce the new generating vector $(1,0,0,0,0,0,0,0)$ to obtain a 9-length code E_1 over $\mathbb{Z}_4$ with 5 generators. It can be verified that the minimum PR' of all the cosets of E_1 is 5 and there are three cosets of E_1 with $PR' = 5$.

4. A Special Type of Lengthening

In this section, we show the importance of some particular type of lengthening which is useful in the study of $PMEPR$. From a given r rather from a given $RM_2(1,r)$, we can obtain $(r+1)^{(r+1)}$ linear codes of double length such that each of the linear codes have at least $d^2 2^k$ cosets with $PMEPR$ less than or equal to 4, where d is the number of cosets of $RM_2(1,r)$ whose $PMEPR$ is less than or equal to 2.

Starting from a q-ary (n, q^k, d) coset-code of $PMEPR$ m, a q-ary $(2n, q^{2k}, 2d)$ coset-code of $PMEPR$ atmost $2m$ has been achieved in this paper.

Now we describe what we exactly mean by lengthening and by lengthening we always mean this particular type of lengthening which we are going to describe now and we are going to say this particular type of lengthening as side by side lengthening.

Definition 2 — Let, S be a binary linear $[n,k]$ code and let $\{e_1, e_2, \ldots, e_k\}$ be the basis of S. Now, if, $x_1 = (y_1, y_2, \ldots, y_n)$ and $x_2 = (y'_1, y'_2, \ldots, y'_n)$ are two binary words of length n, then by x_1x_2 we mean $(y_1, y_2, \ldots, y_n, y'_1, y'_2, \ldots, y'_n)$. Now let S_1 be the binary linear $[2n,k]$ code that has $\{e_1e_{i_1}, e_2e_{i_2}, \ldots, e_ke_{i_k}\}$ or $\{e_{i_1}e_1, e_{i_2}e_2, \ldots, e_{i_k}e_k\}$ as a basis where $i_1, i_2, \ldots, i_k \in \{1,2,\ldots,k\}$. Then we say S_1 is the side by side lengthening of S.

Note that though the above mentioned process is a particular type of lengthening, but in this paper we mention the above process as lengthening.

Now we state an interesting theorem of this paper.

Theorem 16 — *Let S be a q-ary ($q = p^l$ for some prime p) linear $[n,k]$ code generated by $\{e_1 = (e_{11}, e_{12}, \ldots, e_{1n}), e_2 = (e_{21}, e_{22}, \ldots, e_{2n}), \ldots, e_k = (e_{k1}, e_{k2}, \ldots, e_{kn})\}$ and S_1 be a side by side lengthening of S. Let C_1 and C_2 be two cosets of S with $PMEPR$ less than or equal to 2. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ respectively be the coset representative of C_1 and C_2. Then the $PMEPR$ of the coset of S_1 which has $\alpha\beta$ as the coset representative has to be*

less than or equal to 4. This is true if one takes $\mathbb{Z}_m$ instead of $\mathbb{F}_q$. Moreover, from S we can find at-least k^k lengthening by changing the basis (*for q-ary case*).

PROOF: We will prove the theorem for $\mathbb{F}_q$. The proof over $\mathbb{Z}_m$ is similar.

Without loss of generality, let S_1 is generated by $\{e_1e_{i_1}, e_2e_{i_2}, \ldots, e_ke_{i_k}\}$. Let C be the coset of S_1 such that $\alpha\beta \in C$. Now to complete the proof, we only need to show that $PMEPR$ of C is less than or equal to 4. Now let us take any $(\gamma_1, \gamma_2, \ldots, \gamma_n, \delta_1, \delta_2, \ldots, \delta_n) \in C$, let, $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ and $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$.

Then,

$$\begin{aligned} & (\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n) - (\gamma_1, \gamma_2, \ldots, \gamma_n, \delta_1, \delta_2, \ldots, \delta_n) \in S_1 \\ \text{i.e,} \quad & (\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n) - (\gamma_1, \gamma_2, \ldots, \gamma_n, \delta_1, \delta_2, \ldots, \delta_n) \\ = \quad & c_1(e_{11}, e_{12}, \ldots, e_{1n}, e_{i_11}, e_{i_12}, \ldots, e_{i_1n}) + c_2(e_{21}, e_{22}, \ldots, e_{2n}, e_{i_21}, e_{i_22}, \ldots, e_{i_2n}) + \\ & \ldots + c_k(e_{k1}, e_{k2}, \ldots, e_{kn}, e_{i_k1}, e_{i_k2}, \ldots, e_{i_kn}) \end{aligned}$$

where $c_i \in \mathbb{F}_q$.

Therefore, $(\alpha_1, \alpha_2, \ldots, \alpha_n) - (\gamma_1, \gamma_2, \ldots, \gamma_n) = c_1(e_{11}, e_{12}, \ldots, e_{1n}) + c_2(e_{21}, e_{22}, \ldots, e_{2n}) + \ldots + c_k(e_{k1}, e_{k2}, \ldots, e_{kn})$ i.e $(\alpha_1, \alpha_2, \ldots, \alpha_n) - (\gamma_1, \gamma_2, \ldots, \gamma_n) \in S$ i.e α and γ lie in the same coset of S i.e, $\gamma \in C_1$ and similarly we can show that $\delta \in C_2$. Hence,

$$\begin{aligned} & PR'(\gamma\delta) \\ = \quad & \max_{|z|=1} |(-1)^{\gamma_1} + (-1)^{\gamma_2} z + \ldots + (-1)^{\gamma_n} z^{n-1} + (-1)^{\delta_1} z^n + \ldots + (-1)^{\delta_n} z^{2n-1}| \\ \leq \quad & \max_{|z|=1} |(-1)^{\gamma_1} + (-1)^{\gamma_2} z + \ldots + (-1)^{\gamma_n} z^{n-1}| + \max_{|z|=1} |(-1)^{\delta_1} z^n + \ldots + (-1)^{\delta_n} z^{2n-1}| \\ = \quad & \max_{|z|=1} |(-1)^{\gamma_1} + (-1)^{\gamma_2} z + \ldots + (-1)^{\gamma_n} z^{n-1}| + \max_{|z|=1} |z^n((-1)^{\delta_1} + (-1)^{\delta_2} z + \ldots + (-1)^{\delta_n} z^{n-1})| \\ \leq \quad & \max_{|z|=1} |(-1)^{\gamma_1} + (-1)^{\gamma_2} z + \ldots + (-1)^{\gamma_n} z^{n-1}| + \max_{|z|=1} |((-1)^{\delta_1} + (-1)^{\delta_2} z + \ldots + (-1)^{\delta_n} z^{n-1})| \\ \leq \quad & \sqrt{2n} + \sqrt{2n} = 2\sqrt{2n} \end{aligned}$$

Therefore, $PMEPR(\gamma\delta) \leq \frac{(2\sqrt{2n})^2}{2n} = 4$.

Hence, $PMEPR(C) \leq 4$.

We now state a prove an useful proposition that will precisely give a lower bound on the number of cosets of $PMEPR$ less than or equal to 4 of S_1.

Proposition 17 — With the above mentioned notations as given in the definition of side by side

lengthening, S_1 has at least $d^2 2^k$ cosets with $PMEPR$ less than or equal to 4, where d is the number of cosets of S whose $PMEPR$ is less than or equal to 2.

PROOF: There are d cosets of S with $PMEPR$ less than or equal to 2 and each coset of S has 2^k number of elements. Now let $C_1, C_2, \ldots, C_d$ be the cosets of S such that the $PMEPR$ of each of $C_1, C_2, \ldots, C_d$ are less than or equal to 2. Let $\alpha, \beta \in C_1 \sqcup C_2 \sqcup \ldots \sqcup C_d$. Then by using the above theorem, we can easily say that $PMEPR$ of the coset of S_1 whose coset representative is $\alpha\beta$ is less than or equal to 4. Now, we can choose each of α, β in $d2^k$ ways, so we can choose $\alpha\beta$ in $(d2^k)^2$ ways. Now, let, C represents the coset of S_1 whose coset representative is $\alpha\beta$. Now, let $(\gamma_1, \gamma_2, \ldots, \gamma_n, \delta_1, \delta_2, \ldots, , \delta_n) \in C$. Let, $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ and $\delta = (\delta_1, \delta_2, \ldots, , \delta_n)$. It is clear that $\alpha + \gamma, \beta + \delta \in S$. Therefore, $\gamma, \delta \in C_1 \sqcup C_2 \sqcup \ldots \sqcup C_d$ Hence, there are at least $\frac{(d2^k)^2}{2^k} = d^2 2^k$ cosets with $PMEPR$ less than or equal to 4. □

As we have seen in the first section that whenever any binary linear code has two coset with reasonably low $PMEPR$, then by using the joining-coset method, we can get a new super space of the linear code such that the union of the previous two cosets is a coset of the super space. For that reason, if we need to increase the size of the code without much increasing the $PMEPR$, we need to have many cosets with low $PMEPR$ and that why this particular type of lengthening is important in the theory of $PMEPR$.

Proposition 18 — If we take $PMEPR$ of an affine linear code to be m (instead of 2), then by applying side by side lengthening we will get an affine linear code of double length whose $PMEPR$ is less than or equals to $2m$.

Theorem 19 — *Let L be a q ary linear $[n, k, d]$ code. Let $e_1, e_2, \ldots, e_k$ be a basis of L where $e_i = (e_{i1}, e_{i2}, \ldots, e_{in})$. Let the minimum $PMEPR$ of all the cosets of L be m. Let L_l be the $[2n, 2k, 2d]$ linear code whose basis is $\{\hat{e_1} = e_1\bar{0}, \hat{e_2} = e_2\bar{0}, \ldots, \hat{e_k} = e_k\bar{0}, \hat{e_{k+1}} = \bar{0}e_1, \bar{0}e_2, \ldots, \hat{e_{2k}} = \bar{0}e_k\}$ where $\bar{0}$ is the zero vector of length n. Then L_l has a coset whose $PMEPR$ is less than or equals to $2m$.*

PROOF: Let $c = (c_1, c_2, \ldots, c_n)$ be a coset representative of the coset of L whose $PMEPR$ is m. Let C be that coset of L. Let C_l be the coset of L_l whose coset representative is $cc = (c_1, c_2, \ldots, c_n, c_1, c_2, \ldots, c_n)$. Now, let us take any vector $d = (d_1, d_2, \ldots, d_{2n}) \in C_l$. Then, $d - c \in L_l$. Then $d - c = \sum_{i=1}^{2k} x_i \hat{e_i}$ where $x_i \in \mathbb{F}_q$. Then, it is clear that $(d_1 - c_1, d_2 - c_2, \ldots, d_n - c_n) \in L$ and $(d_{n+1} - c_1, d_{n+2} - c_2, \ldots, d_{2n} - c_n) \in L$ and hence $(d_1, d_2, \ldots, d_n) \in C$ and $(d_{n+1}, d_{n+2}, \ldots, d_{2n}) \in C$. Hence it is easy to calculate that $PMEPR(d) \leq 2m$. Now, since we have chosen $d \in C_l$ arbitrarily, therefore $PMEPR(C_l) \leq 2m$. This completes the proof. □

The proof of the following corollary is similar to the above theorem.

Corollary 20 — Let L be a q-ary linear $[n, k, d]$ code which has a coset of $PMEPR\, m$. Let r be a positive integer. Then there exists a q-ary linear $[rn, rk, rd]$ code L_l which has a coset whose

$PMEPR$ is less than or equals to rm.

Example 4 — (Continuation of Example 1) In this section, we give examples of lengthening of binary linear codes such that each of the binary linear codes has a coset of $PMEPR$ less than or equal to 2. If S is a binary linear $[n, k]$ code such that it has a coset with $PMEPR$ less than or equal to 2 and if S_1 is the lengthening of S, then by proposition 2, S_1 has $d^2 2^k$ cosets with $PMEPR$ less than or equal to 4 (where d is the number of cosets of S with $PMEPR$ less than equal to 2) and hence one can expect that some coset of S_1 can be less than or equal to 2 and indeed, we have found that in some cases and moreover if we start with $S = RM_2(1, r)$ then $S_1 \subset RM_2(1, r + 1)$.

We have computed $PMEPR$ of several linear codes (over $\mathbb{F}_2$) and all it's cosets.

1. In this case we take $S = RM_2(1, 3)$ and $i_j = j$ for all $j = 1, 2, \ldots, k$. Then it is clear that $S_1 \subset RM_2(1, 4)$. As it is clear that this code is a sub code of $RM_2(1, 4)$, therefore it has cosets of $PMEPR$ less than or equals to 2.

2. Let, L_2 be the binary linear code generated by $\{(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$, $(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1), (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1), (1, 1, 1, 1,$ $1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)\}$. Then, it is clear that L_2 is a side by side lengthening of $RM_2(1, 4)$. Now the minimum $PMEPR$ of all the cosets of L_2 is 1.9965. L_2 has 8 cosets of $PMEPR$ less than or equals to 2.

3. Let, L_3 be the binary linear code generated by $\{(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$, $(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$, $(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$, $(1, 1, 1, 1, 1,$ $1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)\}$. Now, it is clear that L_3 is a side by side lengthening of $RM_2(1, 4)$. The minimum $PMEPR$ of all the cosets of L_2 is 1.9855.

ACKNOWLEDGEMENT

This work was partly supported by the DRDO-IISc Program on Advanced Research in Mathematical Engineering and by the Council of Scientific & Industrial Research (CSIR), India, through Research Grant (22(0365)/04/EMR-II) to B.S. Rajan.

The first author gratefully acknowledges CSIR for funding this work by way of Research Fellowship and thankful to Mr Anindya Goswami for his help with Matlab and Mathematica and also for the discussions and constant encouragement.

REFERENCES

1. James A. Davis and Jonathan Jedwab, "Peak-to-Mean Power Control in OFDM, Golay Complementary Sequences, and Reed-Muller Codes," *IEEE Transactions on information theory*, **45**(7) (1999), 2397-2417.

2. Kenneth G. Paterson and Vahid Tarokh, “On the Existence and Construction of Good Codes with Low Peak-to-Average power Ratios,” *IEEE Transactions on information theory*, **46**(6) (2000), 1974-1987.

3. Steven Roman, *Coding and information theory*. Graduate Texts in Mathematics, 134, Springer-Verlag, New York, 1992.

4. Rudolf Lidl, Harald Niederreiter and P. M. Cohn, *Finite Fields*, Cambridge University Press, Cambridge, 1997.