Math. Appl. **4** (2015), 91–99
DOI: 10.13164/ma.2015.07

ON PERTURBATION OF BINARY LINEAR CODES

PANKAJ K. DAS AND LALIT K. VASHISHT

Abstract. We present new codes by perturbation of rows of the generating matrix of a given linear code. Some properties of the perturbed linear codes are given.

1. Introduction and preliminaries

In coding theory, many methods from elementary to more complicated ones are used to construct new codes from one or more given codes. Some examples of such new codes are product code [3], punctured code [6], shortened code [4], and extended code [4]. The new codes are developed in order to obtain a better code in some sense or other. Akavia and Venkatesan [1] presented a new class of perturbation codes that are obtained from old codes using perturbation operator. They analyze the rate and distance of perturbation codes.

In this paper, we discuss a type of perturbation in which the rows v_i of a generator matrix G of an (n, k) linear code C are perturbed by a non-zero vector, i.e.,

$$G +_r u \equiv \begin{bmatrix} v_1 + u \\ v_2 + u \\ \vdots \\ v_k + u \end{bmatrix},$$

where u is a non-zero vector which may or may not be in C. In general, $G +_r u$ does not form a generator matrix of the given linear code. It would be interesting to know whether, the perturbed system $G +_r u$ forms a generator matrix of a linear subcode or under which conditions it generates the original code. In this direction we give necessary and sufficient conditions for the perturbation of linear codes for generating new (or original) linear codes. A decomposition theorem and MacWilliams type identity for the perturbed linear code are given. An error detection and error correction relation between a given linear code and the corresponding perturbed code have been discussed.

Now we give some basic definitions which will be used throughout this paper. The set V^n denotes the space of all n-tuples over a finite field $GF(q)$ (q is a power of some prime number) with the usual inner product $\langle ., . \rangle$. Two vectors x and y in

MSC (2010): primary 94B05; secondary 94B20, 94B65.
Keywords: linear codes, generator matrix, perturbation.
The second author is partly supported by R & D Doctoral Research Programme, University of Delhi, Delhi-110007, India (Grant No.: RC/2014/6820).

V^n are said to be orthogonal if $\langle x, y\rangle = 0$. Any proper subspace C of V^n is called a *linear code* and the elements of C are called *code words* (or *code vectors*). A subspace of V^n with every element being orthogonal to every element of C is also a linear code and known as the *dual code* of C denoted by $C^\perp$. If the dimension of C is k, then C is called an (n, k) *linear code*. A $k \times n$ matrix whose rows span C is called a *generator matrix*. Any generator matrix H of $C^\perp$ is called a *parity check matrix* of C. An (n, k) linear code C over a finite field $GF(q)$ is called a *cyclic code* if, for every code word $v = (v_1, v_2, \ldots, v_n)$ of C, the word $(v_n, v_1, \ldots, v_{n-1})$ obtained by a cyclic shift of components is again a code word.

The *Hamming weight* of a vector is the number of its non-zero components. The Hamming distance between two vectors is the number of components in which they differ. The minimum distance for a linear code equals the minimum weight of its non-zero vectors. The distance of a linear code is the minimum distance of the code.

Recall that, for sets U and W, $U \oplus W$ denote the subspace consisting of all linear combinations $ax + by$ where $x \in U$, $y \in W$ and a, b are scalars. For a set E, $|E|$ denotes the number of elements in E.

2. Perturbation of linear codes

In this section, we perturb a generator matrix of a linear code by a non-zero vector. First we take a non-zero element from the code and call this operation on linear codes an *inner perturbation* of linear codes. The following proposition gives the necessary condition for an inner perturbation of linear codes.

Proposition 2.1. *Let C be a binary (n, k) linear code generated by a matrix*

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}.$$

If each row v_i of G is perturbed by the linear sum of the form $u = \sum_{i=1}^{k} v_i$, then the perturbed matrix

$$G_0 = \begin{bmatrix} v_1 + u \\ v_2 + u \\ \vdots \\ v_k + u \end{bmatrix} \tag{2.1}$$

gives rise to the same linear code C provided that k is even.

Proof. It is sufficient to show that the rows in matrix G_0 are linearly independent. Assume that

$$\alpha_1(v_1 + u) + \alpha_2(v_2 + u) + \alpha_3(v_3 + u) + \cdots + \alpha_k(v_k + u) = 0 \tag{2.2}$$

for some scalars $\alpha_i \in GF(2)$ $(1 \le i \le k)$. Now

$$\begin{aligned} &\alpha_1(v_1 + u) + \alpha_2(v_2 + u) + \alpha_3(v_3 + u) + \cdots + \alpha_k(v_k + u) \\ &\qquad = (\alpha_2 + \alpha_3 + \cdots + \alpha_k)v_1 + (\alpha_1 + \alpha_3 + \cdots + \alpha_k)v_2 + \ldots \end{aligned}$$

$$+ (\alpha_1 + \alpha_2 + \cdots + \alpha_{k-1})v_k.$$

Since v_i's are linearly independent, by (2.2), we have

$$\begin{aligned}
\alpha_2 + \alpha_3 + \cdots + \alpha_k &= 0,\\
\alpha_1 + \alpha_3 + \cdots + \alpha_k &= 0,\\
&\cdots\\
&\cdots\\
\alpha_1 + \alpha_2 + \cdots + \alpha_{k-1} &= 0.
\end{aligned}$$

This yields $\alpha_1 = \alpha_i$ $(2 \le i \le k)$. Thus, $(k-1)\alpha_i = 0$ $(1 \le i \le k)$. If k even, then $\alpha_i = 0$. The proposition is proved. □

Remark 2.2. The result given in Proposition 2.1 is not true for odd values of k. Indeed, let C be a $(6, 3)$ linear code with generator matrix

$$\mathcal{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 1 & 0 & 1 & 0\\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Choose $u = (100011)$ $\left(= \sum_{i=1}^{3} v_i\right)$. Then, the perturbed matrix (in the sense of (2.1)) is given by

$$\mathcal{G}_0 = \begin{bmatrix} v_1 + u\\ v_2 + u\\ v_3 + u \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1\\ 1 & 1 & 1 & 0 & 0 & 1\\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

One may observe that the sum of the first two rows in $\mathcal{G}_0$ is equal to the third row in $\mathcal{G}_0$. Hence, the perturbed matrix $\mathcal{G}_0$ cannot be a generator matrix of the given code C. More precisely, the idea given in the above example can be generalized to any (n, k) linear code where n is arbitrary and k is odd.

The following proposition provides a subcode with distance increased by an inner perturbation.

Proposition 2.3. *Assume that d is the distance of an (n, k) binary cyclic linear code C generated by the matrix*

$$G = \begin{bmatrix} v_1\\ v_2\\ \vdots\\ v_k \end{bmatrix} \quad \textit{where } v_j \textit{ is cyclic shift of } v_{j-1} \textit{ for all } j \textit{ with } 2 \le j \le k.$$

If the weight of $v_1 = d$ and d is odd, then the perturbed matrix

$$G_0 = \begin{bmatrix} v_1 + u\\ v_2 + u\\ \cdots\\ v_{i-1} + u\\ v_{i+1} + u\\ \cdots\\ v_k + u \end{bmatrix} \quad \textit{where } u = v_i \textit{ for some } i \textit{ with } 1 \le i \le k, \tag{2.3}$$

generates an $(n, k-1)$ *binary linear subcode of a distance greater than or equal to* $d+1$.

Proof. First we note that the rows of matrix G_0 (see (2.3)) are linearly independent, so G_0 generates an $(n, k-1)$ linear subcode C_1 of C. Since all the row code vectors in G are of odd weight, therefore, all the row code vectors in G_0 are of an even weight. Also, the linear sum of vectors of even weight will produce vector of an even weight. Hence, all code vectors of C_1 are of even weights. Since the minimum weight of C is d which is odd and C_1 is a subcode of C, the minimum distance of $C_1 \geq d+1$. □

The next result provides a necessary condition for a perturbation of a given linear code in terms of an eigenvalue of a certain matrix.

Theorem 2.4. *Assume that* C *is a binary* (n, k) *linear code generated by a matrix*

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}.$$

Let $z_1, z_2, \ldots, z_m$ *be linearly independent vector in* C *and let, for each* j $(1 \leq j \leq m)$, x_j *be vectors* (*not necessarily code vectors*) *with binary components and let* $\alpha_j^{(i)}$ *be scalars given by* $\alpha_j^{(i)} = \langle v_i, x_j \rangle$ *for all* i *with* $1 \leq i \leq k$. *If the perturbed matrix*

$$G_p = \begin{bmatrix} v_1 + \sum_{j=1}^{m} \alpha_j^{(1)} z_j \\ v_2 + \sum_{j=1}^{m} \alpha_j^{(2)} z_j \\ \vdots \\ v_k + \sum_{j=1}^{m} \alpha_j^{(k)} z_j \end{bmatrix}$$

is a generator of C, *then* $\lambda = \pm 1$ *is not an eigenvalue of the matrix*

$$L = \begin{bmatrix} \langle z_1, x_1 \rangle & \langle z_1, x_2 \rangle & \ldots & \langle z_1, x_m \rangle \\ \langle z_2, x_1 \rangle & \langle z_2, x_2 \rangle & \ldots & \langle z_2, x_m \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle z_m, x_1 \rangle & \langle z_m, x_2 \rangle & \ldots & \langle z_m, x_m \rangle \end{bmatrix}.$$

Proof. We prove the theorem for the case $m = 2$ and $\lambda = 1$. The other cases can be proved similarly. Assume that 1 is an eigenvalue of the matrix

$$J_2 = \begin{bmatrix} \langle z_1, x_1 \rangle & \langle z_1, x_2 \rangle \\ \langle z_2, x_1 \rangle & \langle z_2, x_2 \rangle \end{bmatrix}.$$

Then

$$\begin{vmatrix} \langle z_1, x_1 \rangle - 1 & \langle z_1, x_2 \rangle \\ \langle z_2, x_1 \rangle & \langle z_2, x_2 \rangle - 1 \end{vmatrix} = 0.$$

Therefore, we can find scalars α and β not both zero ($\alpha, \beta \in GF(2)$) such that

$$\alpha \langle z_1, x_1 \rangle + \beta \langle z_1, x_2 \rangle = \alpha$$

and

$$\alpha\langle z_2, x_1\rangle + \beta\langle z_2, x_2\rangle = \beta.$$

Put $z = \alpha x_1 + \beta x_2$. Then, z is a non-zero vector.

By using

$$\langle v_i, z\rangle = \langle v_i, \alpha x_1 + \beta x_2\rangle = \alpha\alpha_1^{(i)} + \beta\alpha_2^{(i)} \text{ for all } i \ (1 \le i \le k),$$

we compute

$$\begin{aligned}\langle v_i + \sum_{j=1}^{2} \alpha_j^{(i)} z_j, z\rangle &= \langle v_i, z\rangle + \alpha_1^{(i)}\langle z_1, z\rangle + \alpha_2^{(i)}\langle z_2, z\rangle \\ &= (\alpha\alpha_1^{(i)} + \beta\alpha_2^{(i)}) + \alpha_1^{(i)}\alpha + \alpha_2^{(i)}\beta \\ &= 0, \ (1 \le i \le k). \end{aligned} \tag{2.4}$$

By the hypothesis, G_p is the generator matrix of the given code C. Therefore, the zero vector is only code vector which is orthogonal to all rows that appear in G_p. Hence, by using (2.4), we conclude that $z = 0$, a contradiction. Therefore, 1 is not an eigenvalue of matrix J_2. □

Application of Theorem 2.4: Consider the generator matrix G of a linear $(7, 3)$ code C:

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}.$$

Choose $z_1 = x_1 = v_1; z_2 = x_2 = v_2$. Then,

$$\langle z_1, x_1\rangle = 1, \ \langle z_1, x_2\rangle = 0; \ \langle z_2, x_1\rangle = 0, \ \langle z_2, x_2\rangle = 1.$$

Therefore, -1 is an eigenvalue of the matrix

$$J_2 = \begin{bmatrix} \langle z_1, x_1\rangle & \langle z_1, x_2\rangle \\ \langle z_2, x_1\rangle & \langle z_2, x_2\rangle \end{bmatrix}.$$

Hence, by Theorem 2.4 the matrix

$$G_p = \begin{bmatrix} v_1 + \sum_{k=1}^{2} \alpha_k^{(1)} z_k \\ v_2 + \sum_{k=1}^{2} \alpha_k^{(2)} z_k \\ v_3 + \sum_{k=1}^{2} \alpha_k^{(3)} z_k \end{bmatrix}$$

is not a generator of the given code C.

The case of outer perturbation: Now we discuss the case $G +_r u$ where $u \notin C$. First, we give a result which gives a link between the cardinality of a given linear code and the corresponding outer perturbed code.

Proposition 2.5. *Let C be a binary (n, k) linear code generated by a matrix*

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}.$$

Let u be a non-zero vector which is not in C and let C' be the binary linear code generated by the perturbed matrix

$$G_u = \begin{bmatrix} v_1 + u \\ v_2 + u \\ \vdots \\ v_k + u \end{bmatrix}.$$

Then, $|C \bigcap C'| = \frac{1}{2}|C| = \frac{1}{2}|C'|$.

Proof. By definition of G_u, one may observe that

$$\sum_{\text{even number of terms}} (v_j + u) = \sum_{\text{even number of terms}} v_j \in C \tag{2.5}$$

and

$$\sum_{\text{odd number of terms}} (v_j + u) = \left(\sum_{\text{odd number of terms}} v_j \right) + u \notin C. \tag{2.6}$$

Note that the number of ways in which the linear sums in (2.5) can be chosen is

$$\binom{k}{0} + \binom{k}{2} + \binom{k}{4} + \cdots + \binom{k}{l}, \tag{2.7}$$

where $l = k$ (or $k-1$) according to whether k is even or odd.
Similarly, the linear sums in (2.6) can be chosen in

$$\binom{k}{1} + \binom{k}{3} + \cdots + \binom{k}{t} \tag{2.8}$$

ways where $t = k$ (or $k-1$) according to whether k is odd or even.

Since

$$\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \binom{k}{3} + \cdots + \binom{k}{k} = 2^k$$

and

$$\binom{k}{0} + \binom{k}{2} + \binom{k}{4} + \cdots + \binom{k}{l} = \binom{k}{1} + \binom{k}{3} + \binom{k}{5} + \cdots + \binom{k}{t},$$

where l and t are as above. Therefore, by using (2.7) and (2.8), we have

$$\binom{k}{0} + \binom{k}{2} + \binom{k}{4} + \cdots + \binom{k}{l} = 2^{k-1}.$$

Therefore, the number of elements which are common to both C and C' is equal to 2^{k-1}. Hence $|C \bigcap C'| = \frac{1}{2}|C| = \frac{1}{2}|C'|$. □

Remark 2.6. One may observe that the doping vector u in Proposition 2.5 is not a code vector of C'.

Remark 2.7. One can verify the symmetric relation:

$$(C' + u) \bigcup C' = (C + u) \bigcup C.$$

Remark 2.8. The dimension of $(C \oplus C')$ is $k+1$. Note that $\dim(C \bigcap C') = k-1$ and $\dim C + \dim C' = 2k$. By using the relation

$$\dim(C \bigcap C') + \dim(C \oplus C') = \dim C + \dim C',$$

we have $\dim(C \oplus C') = k + 1$.

The following theorem provides a decomposition of an outer perturbed code in terms of a linear subcode and a nonlinear code.

Theorem 2.9. (Decomposition Theorem) *Let C' be the binary (n, k) linear code given in Proposition* 2.5. *Then C' can be decomposed as an $(n, k-1)$ linear code A and a nonlinear code B.*

Proof. Choose

$$A = \sum_{\text{even number of terms}} (v_j + u) = \sum_{\text{even number of terms}} v_j,$$

and

$$B = \sum_{\text{odd number of terms}} (v_j + u).$$

Then, $C' = A \bigcup B$ and $A \bigcap B = \emptyset$.

To show that A is an $(n, k-1)$ linear code, it is sufficient to show that the matrix G_0 generates A where

$$G_0 = \begin{bmatrix} v_1 + v_2 \\ v_2 + v_3 \\ \vdots \\ v_{k-1} + v_k \end{bmatrix}.$$

Let $\alpha_1(v_1 + v_2) + \alpha_2(v_1 + v_2) + \cdots + \alpha_{k-1}(v_{k-1} + v_k) = 0$, where $\alpha_i \in GF(2)$. Then, $\alpha_1 v_1 + (\alpha_1 + \alpha_2)v_2 + \cdots + (\alpha_{k-2} + \alpha_{k-1})v_{k-1} + \alpha_{k-1}v_k = 0$. By using the linear independence of v_i, we have $\alpha_j = 0$, for all $j = 1, 2, \ldots, k-1$. Furthermore, by the nature of the construction of A, we observe that G_0 spans A. Hence, G_0 is a generator matrix of A. Thus, A is an $(n, k-1)$ linear code. One may observe that B is a nonlinear code. The theorem is proved. □

The following proposition gives a relation of the weight distribution between the subspace A of C' and the null spaces $C^{\perp}$(*or* $C'^{\perp}$). We use certain ideas developed in [2].

Proposition 2.10. *Assume that $A \bigcup B$ is the decomposition of C' given in Theorem 2.9. Let A_i and B_i be the number of vectors of weight i in A and the null space $C^{\perp}$(or $C'^{\perp}$), respectively. Then*

$$\sum_{i=0}^{n} A_i \binom{n-i}{m} \geq 2^{k-1-m} \sum_{j=0}^{n} B_j \binom{n-j}{n-m}, \quad m = 1, 2, \ldots n.$$

Proof. Consider the $(n, k-1)$ linear code A. Applying MacWilliams identity (see Theorem 3.14 in [5]) to the code A, the weight enumerator of A is given by

$$\sum_{i=0}^{n} A_i \binom{n-i}{m} = 2^{k-1-m} \sum_{j=0}^{n} D_j \binom{n-j}{n-m}, \quad m = 1, 2, \ldots n, \tag{2.9}$$

where D_i is the total number of vectors of weight i in $A^{\perp}$.

Now $A \subset C(\text{or } C')$, i.e., $C^{\perp}$ (or $C'^{\perp}$) $\subset A^{\perp}$. Thus, $B_i \leq D_i$. Therefore, by using (2.9), we have

$$\sum_{i=0}^{n} A_i \binom{n-i}{m} \geq 2^{k-1-m} \sum_{j=0}^{n} B_j \binom{n-j}{n-m}.$$

□

Correction and detection of errors: Now we discuss the error detection and error correction relation between a given linear code and the corresponding outer perturbed code.

Proposition 2.11. *If C is a binary (n, k) cyclic linear code, then A (where A is given in the proof of Theorem 2.9) can detect any burst of length $n-k+1$ or less.*

Proof. First we show that A is an $(n, k-1)$ cyclic linear code. Let C be generated by the generator polynomial $g(x)$. By Theorem 2.9, the generator matrix G_0 of A is given by

$$G_0 = \begin{bmatrix} g(x) + xg(x) \\ xg(x) + x^2 g(x) \\ \vdots \\ x^{k-1}g(x) + x^k g(x) \end{bmatrix}$$

$$= \begin{bmatrix} (1+x)g(x) \\ x(1+x)g(x) \\ \vdots \\ x^{k-2}(1+x)g(x) \end{bmatrix}.$$

This shows that A is generated by $(1+x)g(x)$ and, hence, A is a binary $(n, k-1)$ cyclic code.

Since an (n, k) cyclic code detects all burst of length $n-k$ or less, see Theorem 8.5 in [5, p. 229], A detects all burst of length $n-k+1$ or less. □

To conclude the paper, we will prove a result regarding the perturbation in the correction of an error vector.

Proposition 2.12. *Let C be a binary (n, k) linear code which can correct error sets E and $E+u$ $(= \{t+u : t \in E\})$. Then, C' also corrects error sets E and $E+u$.*

Proof. Let e_1, e_2 be any two error vectors in E or of the form $t+u$ $(t \in E)$. To prove that C' corrects error sets E and $E+u$, it is sufficient to show that e_1 and e_2 are members of two different cosets of C'. Let, if possible, e_1, e_2 be members of the same coset of C'. Then, $e_1 - e_2$ must be a code vector of C'. Therefore, $e_1 - e_2 \in A$ or B.

If $e_1 - e_2 \in A$, then $A + e_1 = A + e_2$. This means that $(C + e_1) \bigcap (C + e_2) \neq \phi$, i.e., $C + e_1 = C + e_2$. By using the fact that $e_1 \in C + e_1$ and $e_2 \in C + e_2$ and that C corrects e_1 and e_2, we have $C + e_1 \neq C + e_2$. This is a contradiction. If $e_1 - e_2 \in B$, then $e_1 - e_2 + u \in C$. That is, $C + e_1 = C + e_2 + u$. As C corrects e_1 and $e_2 + u$ and that $e_1 \in C + e_1$ and $e_2 + u \in C + e_2 + u$, then $C + e_1 = C + e_2 + u$ is not possible. Hence, e_1 and e_2 must be members of two different cosets of C'. □

Acknowledgment. The authors would like to thank the anonymous reviewer for his/her careful reading of the paper and valuable comments and suggestions to improve the quality of the paper.

References

[1] A. Akavia and R. Venkatesan, *Perturbation codes*, Presented at IPAM Workshop on Locally Decodable Codes, 2006.

[2] E. F. Assmus (Jr.) and H. F. Mattson (Jr.), *The weight-distribution of a coset of a linear code*, IEEE Trans. Inf. Theory **24** (1978), 497–497.

[3] P. Elias, *Error-free coding*, Information Theory, Transactions of the IRE Professional Group on **4** (1954), 29–37.

[4] S. J. K. Kenneth, *Construction of binary linear codes*, Undergraduate Research Opportunity Programme in Science, Department of Mathematics, National University of Singapore, 1999/2000 (`www.math.nus.edu.sg/ urops/Projects/BinaryCodes`)

[5] W. W. Peterson and E. J. Weldon (Jr.), *Error-Correcting Codes*, 2nd ed., The MIT Press, 1972.

[6] H. van Tilborg, *Coding Theory: A First Course*, Eindhoven the Netherlands, 1993.

Pankaj K. Das, Department of Mathematics, Shivaji College, University of Delhi, Raja Garden, New Delhi–110027, India (Presently on lien in Department of Mathematical Sciences, Tezpur University, Napaam, Sonitpur, Assam–784 028, India)
e-mail: `pankaj4thapril@yahoo.co.in, pankaj4@tezu.ernet.in`

Lalit K. Vashisht, Department of Mathematics, University of Delhi, Delhi–110007, India
e-mail: `lalitkvashisht@gmail.com`