International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452 Maths 2018; 3(2): 45-47 © 2018 Stats & Maths
www.mathsjournal.com
Received: 15-01-2018
Accepted: 23-02-2018

Anita Pruthi
PG Department of Mathematics, D.A.V. College, Abohar, Punjab, India

Corresponding Author:
Anita Pruthi
PG Department of Mathematics, D.A.V. College, Abohar, Punjab, India

On the property of properness in the extended triple-error-correcting BCH codes

Anita Pruthi

DOI: https://doi.org/10.22271/maths.2018.v3.i2a.602

Abstract
The undetected error probability $p_u(\varepsilon)$ for the primitive triple-error-correcting BCH codes of blocklength $2^m - 1$ on a BSC with cross-over probability $\varepsilon \leq 1/2$ has been widely studied. In this correspondence, extended triple-error-correcting BCH codes of blocklength 2^m are studied and the results presented in are supported and strengthened but with a different approach i.e., it is proved that the extended triple-error-correcting BCH codes of blocklength 2^m don't satisfy the properties of proper codes for even $m \geq 6, m$ integer.

Keywords: Proper codes, undetected error probability

1. Introduction
Proper codes are studied extensively, specifically in [3]. Performance of proper codes is good in error controlling. A code is said to be proper if its undetected error probability $p_u(\varepsilon)$ is an increasing function of ε. Proper codes perform good in error control [4]. When a codeword from a code is transmitted over a channel and some error occurs during transmission and if the received vector is not a codeword then errors are detected. But it may also happen than errors are so combined that the received vector is also one of the codewords. In such a case there is no way to detect that received codeword is not the sent codeword and in this way there arises an undetected error.

2. Claim: The extended triple-error-correcting BCH codes of blocklength 2^m are not proper for even $m \geq 6, m$ integer**.**

3. Proof: For a code to be proper its undetected error probability $p_u(\varepsilon)$ should increase as ε (Bit error rate) increases.
Now $p_u(\varepsilon)$ for an (n, k) code can be calculated from the weight distribution of its dual by using the MacWilliams identity and its expression is given by
$p_u(\varepsilon) = 2^{-(n-k)} B(1-2p) - (1-p)^n$,

where $(1-2p) = \sum_{i=0}^{n} B_i (1-2p)^i$, $B_i, 0 \leq i \leq n,$ represents weight distribution of dual code, p is the transition probability of the BSC.
Although, $p_u(\varepsilon)$ can be calculated not only by the wright distribution of the dual of the code but also by the weight distribution of the code itself. So in this claim, $p_u(\varepsilon)$ is calculated by using weight distribution of the dual of extended triple-error-correcting BCH codes of Blocklength 2^m.
The weight distribution [5] of the dual of the code is as follows:

Weight i	Number of Vectors B_i
$0, 2^m$	1
$2^{m-1} \pm 2^{(m+2)/2}$	$2^m(2^m-1)(2^m-4)/960$
$2^{m-1} \pm 2^{m/2}$	$7.2^m(2^m-1)/48$
$2^{m-1} \pm 2^{(m-2)/2}$	$2.2^m(2^m-1)(3.2^m+8)/15$

2^{m-1} $(2^m-1)(29.2^{2m}-4.2^m+64)/32$

Putting $l=2^{(m-2)/2}$ and $p=3m+1$ we have

$$p_u(\varepsilon)=2^{-3m-1}\sum_{i=0}^{n}B_i\,(1-2\varepsilon)^i-(1-\varepsilon)^n$$

$$=\frac{1}{128l^6}\Big\{\left[1+1(1-2\varepsilon)^{2^m}\right]+(1-2\varepsilon)^{2^{m-1}+2^{(m+2)/2}}[2^m(2^m-1)(2^m-4)/960]+(1-2\varepsilon)^{2^{m-1}-2^{(m+2)/2}}[2^m(2^m-1)(2^m-4)/960]+(1-2\varepsilon)^{2^{m-1}+2^{m/2}}[7.2^{2m}(2^m-1)/48]+(1-2\epsilon)^{2^{m-1}-2^{m/2}}[7.2^{2m}(2^m-1)/48]+(1-2\varepsilon)^{2^{m-1}+2^{(m-2)/2}}[2.2^m(2^m-1)(3.2^m+8)/15]+(1-2\varepsilon)^{2^{m-1}-2^{(m-2)/2}}[2.2^m(2^m-1)(3.2^m+8)/15]+(1-2\varepsilon)^{2^{m-1}}[(2^m-1)(29.2^{2m}-4.2^m+64)/32]\Big\}-(1-\varepsilon)^{2^m}$$

$$=\frac{1}{128l^6}\Big\{\left[1+1(1-2\varepsilon)^{4l^2}\right]+(1-2\varepsilon)^{2l^2+4l}[4l^2(4l^2-1)(4l^2-4)/960]+(1-2\varepsilon)^{2l^2-4l}[4l^2(4l^2-1)(4l^2-4)/960]+(1-2\varepsilon)^{2l^2+2l}[7.16l^4(4l^2-1)/48]+(1-2\epsilon)^{2l^2-2l}[7.16l^4(4l^2-1)/48]+(1-2\varepsilon)^{2l^2+l}[2.4l^2(4l^2-1)(3.4l^2+8)/15]+(1-2\varepsilon)^{2l^2-l}[2.4l^2(4l^2-1)(3.4l^2+8)/15]+(1-2\varepsilon)^{2l^2}[(4l^2-1)(29.16l^4-4.4l^2+64)/32]\Big\}-(1-\varepsilon)^{4l^2} \quad \text{(i)}$$

On differentiating $p_u(\varepsilon)$ w.r.t.,

$$\frac{d}{d\varepsilon}p_u(\varepsilon)=\frac{-2}{128l^6}\Big\{4l^2(1-2\varepsilon)^{4l^2-1}+[4l^2(4l^2-1)(4l^2-4)/960]\left((2l^2+4l)(1-2\varepsilon)^{2l^2+4l-1}+(2l^2-4l)(1-2\varepsilon)^{2l^2-4l-1}\right)+[7.16l^4(4l^2-1)/48]((2l^2+2l)(1-2\varepsilon)^{2l^2+2l-1}+(2l^2-2l)(1-2\varepsilon)^{2l^2-2l-1})+[2.4l^2(4l^2-1)(3.4l^2+8)/15]((2l^2+l)(1-2\varepsilon)^{2l^2+l-1}+(2l^2-l)(1-2\varepsilon)^{2l^2-l-1})+[(4l^2-1)(29.16l^4-4.4l^2+64)/32]2l^2(1-2\varepsilon)^{2l^2-1}\Big\}+4l^2(1-\varepsilon)^{4l^2-1}$$

$$=\frac{-1}{64l^4}\Big\{(1-2\varepsilon)^{4l^2-1}+[(4l^2-1)(4l^2-4)/960]\left((2l^2+4l)(1-2\varepsilon)^{2l^2+4l-1}+(2l^2-4l)(1-2\varepsilon)^{2l^2-4l-1}\right)+[7.4l^2(4l^2-1)/48]((2l^2+2l)(1-2\varepsilon)^{2l^2+2l-1}+(2l^2-2l)(1-2\varepsilon)^{2l^2-2l-1})+[2(4l^2-1)(3.4l^2+8)/15]((2l^2+l)(1-2\varepsilon)^{2l^2+l-1}+(2l^2-l)(1-2\varepsilon)^{2l^2-l-1})+[(4l^2-1)(29.8l^2-8l^2+32)/32](1-2\varepsilon)^{2l^2-1}\Big\}+4l^2(1-\varepsilon)^{4l^2-1} \quad \text{(iii)}$$

Using Equations (i) and (ii), we have the following table:-

Table 1: Values of undetected error probability $p_u(\varepsilon)$ for given ε, for $6\le m\le 16$.

S. No.	m	l	ε	$p_u(\varepsilon)$	$d/_{d\varepsilon}\,p_u(\varepsilon)$
1.	6	4	0.1	9.837993990569e-07	-8.250700739498e-02
			0.2	1.918934366274e-06	-4.945716694417e-05
			0.3	1.907454876543e-06	-1.898542817751e-08
			0.4	1.907348626480e-06	-4.937333414117e-13
			0.5	1.907348632812e-06	1.084202172486e-19
2.	8	8	0.1	2.980232365649e-08	-5.470128317751e-10
			0.2	2.980232238770e-08	-8.624408683311e-23
			0.3	2.980232238770e-08	-1.222599721827e-39
			0.4	2.980232238770e-08	-8.834101051736e-184
			0.5	2.980232238770e-08	0.000000000000e+00
3.	10	16	0.1	4.656612873077e-10	-2.212545631085e-44
			0.2	4.656612873077e-10	-1.066902703526e-233
			0.3	4.656612873077e-10	0.0
			0.4	4.656612873077e-10	0.0
			0.5	4.656612873077e-10	0.0

4.	12	32	0.1	7.275957614183e-12	0.0
			0.2	7.275957614183e-12	0.0
			0.3	7.275957614183e-12	0.0
			0.4	7.275957614183e-12	0.0
			0.5	7.275957614183e-12	0.0
5.	14	64	0.1	1.136868377216e-13	0.0
			0.2	1.136868377216e-13	0.0
			0.3	1.136868377216e-13	0.0
			0.4	1.136868377216e-13	0.0
			0.5	1.136868377216e-13	0.0
6.	16	128	0.1	1.776356839400e-15	0.0
			0.2	1.776356839400e-15	0.0
			0.3	1.776356839400e-15	0.0
			0.4	1.776356839400e-15	0.0
			0.5	1.776356839400e-15	0.0

Table 2: Comparison of $p_u(\varepsilon_{max})$ and 2^{-p}

m	$p_u(\varepsilon_{max})$	2^{-p}
6	1.907348632812446e-06	1.907348632812500e-06
8	2.980232238769531e-08	2.980232238769531e-08
10	4.656612873077393e-10	4.656612873077393e-10
12	7.275957614183426e-12	7.275957614183426e-12
14	1.136868377216160e-13	1.136868377216160e-13
16	1.776356839400250e-15	1.776356839400250e-15

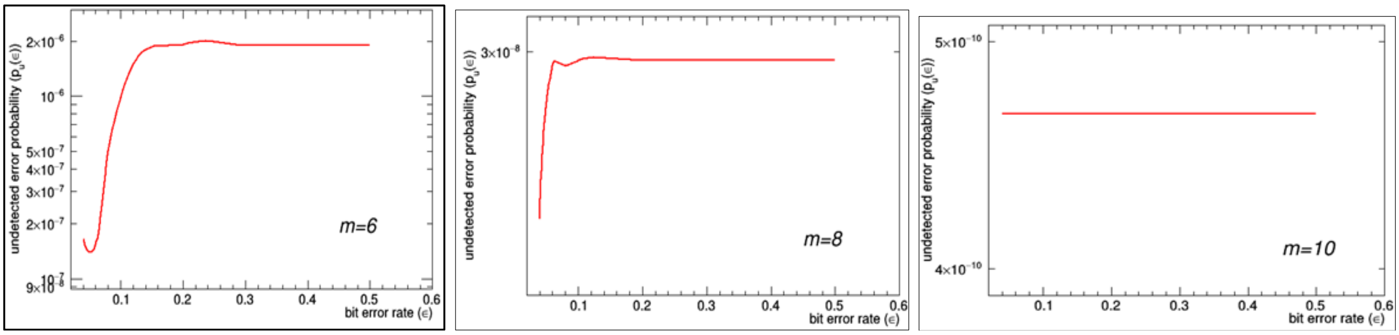

Fig 1: Undetected error probability for $m = 6, 8$ and 10.

4. Conclusion

Table 2 shows that $p_u(\varepsilon)$ doesn't satisfies $p_u(\varepsilon_{max}) < 2^{-p}$ bound except for $m = 6$. For $m = 8, 10, 12, 14, \ldots..$ the bound is exactly equal to $p_u(\varepsilon_{max})$. Also Figure 1 and Table 1 represents that the undetected error probability is not always monotonically increasing as required for proper code. Moreover, for $m \geq 10$, it becomes constant.

Also, on calculating $dp_u(\varepsilon)/d\varepsilon$ is not always found positive for given range of ε and different values of m as shown in Table 1. For$m \geq 12$, as $p_u(\varepsilon)$ attains constant value, $dp_u(\varepsilon)/d\varepsilon$ vanishes. Due to the above mentioned observations, the code doesn't exhibit the property of properness. This completes the proof that the extended primitive triple-error-correcting BCH codes of Blocklength 2^m are not proper for even $m \geq 6, m$ integer.

5. References

1. Ong CT, Leung C. On the undetected error probability of triple-error-correcting BCH codes, IEEE Trans. Inform. Theory 1991;37(3):673-678.
2. Patrick Perry, Necessary condition for good error detection, IEEE Trans. Inform. Theory 1991;37(2):375-378.
3. Leung-Yan-Cheong SK, Barnes ER, Friedman DU. On some properties of the undetected error probability of linear codes, IEEE Trans. Inform. Theory 1979;25(1):110-112.
4. Dodunekova R, Dodunekov SM, Nikolova E, A survey on proper codes, Discrete Applied Mathematics 2008;156(9):1499-1509.
5. Mac Williams, Sloane NJA. Theory of error correcting codes, North-Holland Publishing Company, New York 1977.