RZ 3930 (# ZUR1804-026) 04/13/2018
Electrical Engineering 5 pages

Research Report

Shortened Cyclic Codes for Correcting and Detecting Burst Errors

Roy D. Cideciyan, Simeon Furrer, Mark A. Lantz

IBM Research – Zurich
8803 Rüschlikon
Switzerland

The final version of this article has been published by IEEE: Roy D. Cideciyan ; Simeon Furrer ; Mark A. Lantz "Shortened Cyclic Codes for Correcting and Detecting Burst Errors," Proc. 2018 International Symposium on Information Theory and Its Applications (ISITA)
doi: 10.23919/ISITA.2018.8664370

Shortened Cyclic Codes for Correcting and Detecting Burst Errors

Roy D. Cideciyan*, Simeon Furrer*, and Mark A. Lantz*
*IBM Research-Zurich, 8803 Rüschlikon, Switzerland

***Abstract*—New optimum binary shortened cyclic codes with redundancy $r = 32$ and burst-error correction capability b are presented. The codes are found by performing an exhaustive computer search using the Kasami algorithm, and their performance is compared with analytical bounds by Reiger, Abramson and Campopiano. The true burst-error correction capability of the $[2112, 2080]$ shortened Fire code selected for $10\,\mathrm{Gb/s}$ Ethernet is determined to be $b = 11$ and $[2112, 2080]$ shortened cyclic codes with higher burst-error correction capability $b = 13$ are given. The double burst-error detection properties of three cyclic redundancy check codes used in standards are compared.**

I. Introduction

Many of the well-known error-correcting codes, which are used to correct or detect errors in data transmission and storage, are cyclic or shortened cyclic codes [1], [2]. These codes are an attractive subclass of linear block codes because the operations of encoding and syndrome computation can be performed using linear feedback shift registers (LFSR) and various decoding algorithms can be devised by taking advantage of their rich algebraic structure. Furthermore, while a linear block code can be specified by a parity check matrix with $n(n-k)$ entries where n and k are the length and the dimension of the code, respectively, a shortened cyclic code is completely determined by its generator polynomial $g(x)$ of degree $(n-k)$, which significantly simplifies the task of searching for good codes.

In many communication channels, errors occur in clusters. Burst errors can be corrected by using block or convolutional codes [1], [2]. In this paper, binary block codes of cyclic or shortened cyclic type that correct or detect burst errors are studied. Encoding and decoding for burst-correcting shortened cyclic codes can be accomplished by using simple circuits such as an encoder based on a LFSR and an error-trapping decoder which is a variation of a Meggitt decoder [1], [2]. The most important family of cyclic burst-error correcting codes was developed by Fire [3]. Although it has been known for a long time that the true burst-correction capability of Fire codes can exceed their designed burst-correction capability [4], the true burst-correction capability of various classes of Fire codes was only recently analyzed [5]. However, the family of Fire codes is too small to search for good burst-error correcting codes. In this paper, generator polynomials $g(x)$ of optimum shortened cyclic codes for burst-error correction are found by exhaustive computer search using an efficient algorithm [6] that determines the maximum possible length $n_{\max}$ of a shortened cyclic code with binary generator polynomial $g(x)$ that can correct a burst error of length up to b.

The redundancy $r = (n-k)$ of any $[n, k]$ linear code with burst-error correction capability b is lower bounded by the Reiger bound [7] and the Abramson bound [8], [9] which are well-known in the literature. On the other hand, the Campopiano upper bound on the smallest possible redundancy r for which an $[n, k]$ linear code with burst-error correction capability b exists [10], [11] (see also [1]) has not been used in the search for burst-error correcting codes. In fact, the Campopiano bound has rarely been mentioned in the literature [1], [12], [13]. The Reiger and the Abramson lower bounds in conjunction with the Campopiano upper bound permit the designer of a communication system to evaluate in a simple manner the relative efficacy of a burst-error correcting code. In this paper, the benefits of using all three bounds for the evaluation of specific burst-error correcting and burst-error detecting codes is demonstrated.

In 2007, Ethernet standard IEEE 802.3ap adopted an optional burst-error correcting shortened Fire code with $n = 2112$, $k = 2080$, and a designed burst-error correction capability $b^* = 11$ for backplane transmission at $10\,\mathrm{Gb/s}$ in a printed circuit board [14] (see Section 5, pp. 548-554). One of the goals of this paper is to determine the true burst-error correction capability b of the $[2112, 2080]$ shortened Fire code in IEEE 802.3ap. Another goal of the paper is to determine a generator polynomial $g(x)$ of a $[2112, 2080]$ shortened cyclic code that has the highest burst-error correction capability b. To achieve this, the generator polynomials $g(x)$ of optimum binary shortened cyclic codes with a redundancy of $r = 32$ bits are identified by using an exhaustive computer search for the burst-error correction capabilities $b = 10$ to 16.

In various standards, shortened cyclic codes are pervasively used for error detection. These codes are often referred to as cyclic redundancy check (CRC) codes. Currently, many applications in data transmission and storage use shortened cyclic codes with a fixed redundancy of $r = 32$ bits and a variable information size k, i.e., a variable codeword length n, to detect errors. Byte reordering, error propagation and error multiplication in the receiver can change an error burst into two error bursts. A shortened cyclic code with burst-correction capability b can be used to detect any two error bursts in a codeword where each burst is of length up to b. Fujiwara et al. were first to study the double burst-error detection properties of a CRC code by using the generator polynomial $g(x)$ of the Ethernet CRC code [15]. Their results were extended to determine the double burst-error detection capability of larger jumbo frames in Ethernet [16]. In this paper, the double burst-error detection properties of other CRC codes used in standards are evaluated and compared to each other. Furthermore, we argue that the double burst-error detection capability of a shortened cyclic code should be considered in the selection of a CRC code.

This paper is organized as follows. In Section II, we give various bounds on redundancy and burst correction capability of $[n, k]$ linear codes able to correct a single burst error in a codeword. In Section III, we present new optimum burst-correcting shortened cyclic codes with 32-bit redundancy and determine the true burst-correction capability of the $[2112, 2080]$ shortened Fire code used for $10\,\mathrm{Gb/s}$ Ethernet transmission. Furthermore, we determine the best possible burst-correction capability b that can be achieved by a $[2112, 2080]$ shortened cyclic code. In Section IV, we compare the double burst-error detection properties of various CRC codes used in standards. Section V concludes the paper.

II. Bounds on Redundancy and Burst Correction

In this paper, we consider single (double) error bursts of length up to b in a codeword that can be corrected (detected) by a shortened cyclic code. This type of error bursts is also referred to as open-loop bursts [3], [4], [11] or non-all-around bursts [17]. It is well-known that if a cyclic code can correct all bursts of length up to b in a codeword, it can also correct all cyclic error bursts of length up to b in a codeword [4]. This does not hold for shortened cyclic codes. In the literature, cyclic error bursts [9], [18] are also referred to as wrap-around bursts [19] or closed-loop bursts [3], [4], [11] or all-around bursts [17].

The Reiger bound [7] for an $[n, k]$ linear code with redundancy $r = (n - k)$ and burst-error correction capability b is

$$r \geq 2b \equiv r_{\mathrm{R}}. \tag{1}$$

The Reiger bound is the same for cyclic codes that can also correct cyclic bursts. In the following, $n \geq 2b$ is assumed.

The Abramson lower bound on redundancy [8] (see also [1], [3]) can be tighter than the Reiger bound for a given b and n. For an $[n, k]$ linear code over GF(2) with burst-error correction capability b, the Abramson bound

$$r \geq \lceil b - 1 + \log_2 (n - b + 2) \rceil \equiv r_{\mathrm{A}} \tag{2}$$

is a Hamming-type sphere-packing bound for single burst-error correcting codes. For cyclic codes that can also correct cyclic bursts, the reader is referred to [3], [9]. The Reiger and the Abramson bounds can be combined into one lower bound r_{RA} where $r_{\mathrm{RA}} = \max (r_{\mathrm{R}}, r_{\mathrm{A}})$.

An $[n, k]$ linear code over GF(2) with burst-error correction capability b exists [10] if it satisfies the inequality

$$r > 2(b - 1) + \log_2 (n - 2b + 2)\,. \tag{3}$$

This inequality can be used to show that the smallest possible value of redundancy r for an $[n, k]$ linear code with burst-error correction capability b must satisfy the relation

$$r_{\mathrm{RA}} \leq r \leq r_{\mathrm{C}}, \tag{4}$$

where the Campopiano upper bound on the smallest possible value of redundancy is given by

$$r_{\mathrm{C}} \equiv \lfloor 2(b - 1) + \log_2 (n - 2b + 2) \rfloor + 1. \tag{5}$$

We remark that the Campopiano bound in (5) is tighter than the bound in Theorem 4.17 in [1]. The Campopiano bound is a Varshamov-Gilbert-type bound for single burst-error correcting codes. For cyclic codes that can also correct cyclic bursts it is given in [11].

Extended Hamming-type and Varshamov-Gilbert-type bounds for burst-error correcting codes have been derived by considering the weight of the bursts and the minimum weight of the code [20].

The bounds on redundancy have been specified as a function of b and n. For a given r and n, these bounds translate into corresponding lower and upper bounds b_{R}, b_{A} and b_{C} on the largest possible burst-correction capability b of an $[n, k]$ linear code over GF(2). For example, the Reiger upper bound on b is $b_{\mathrm{R}} = \lfloor r/2 \rfloor$. Although b_{A} and b_{C} cannot be expressed using a closed-form formula, they can readily be computed using the Abramson and Campopiano bounds on redundancy. The Reiger and the Abramson bounds on b can be combined into one upper bound b_{RA} where $b_{\mathrm{RA}} = \min (b_{\mathrm{R}}, b_{\mathrm{A}})$. The largest possible value of b for which an $[n, k]$ linear code over GF(2) exists then satisfies

$$b_{\mathrm{C}} \leq b \leq b_{\mathrm{RA}}. \tag{6}$$

III. New Optimum Shortened Cyclic Codes

There are infinitely many cyclic codes with codeword length n, redundancy r, and burst-error correction capability b which meet the Abramson bound [21]. Various algorithms that determine the burst-error correction capability of cyclic and shortened cyclic codes have been developed. To determine the burst-error correction capability b of a given shortened cyclic code with generator polynomial $g(x)$ and codeword length n, efficient algorithms based on using LFSR synthesis [22] and apolarity of binary forms were developed in [4] and [23], respectively. Furthermore, an efficient and versatile algorithm for searching optimal shortened cyclic codes, which can also correct various types of wrap-around bursts, by using Gray codes to minimize the number of syndrome checks was presented in [24]. In this paper, the Kasami algorithm [6] is used to find new optimum burst-correcting shortened cyclic codes and determine the burst-detection capability of standardized shortened cyclic codes. Specifically, the Kasami algorithm determines the maximum codeword length $n_{\max}$ of a shortened cyclic code for a given b and $g(x)$.

An exhaustive search over all generator polynomials

$$g(x) = g_r x^r + ... + g_1 x + g_0 \tag{7}$$

of degree $r = 32$ and $g_r = g_0 = 1$ was performed for a given burst-error correction capability b where $10 \leq b \leq 16$. As shown in Lemma 5 in [6], the maximum codeword length $n_{\max}$ is identical for two shortened cyclic codes with the same burst-error correction capability b and generator polynomials

$g_1(x)$ and $g_2(x) = g_1(x^{-1})x^r$. Therefore, to speed-up the search, the reciprocal generator polynomials were excluded. Table I lists the maximum codeword length $n_{\max}$ and the generator polynomial $g(x)$ of the optimum shortened cyclic codes that were found. The generator polynomials are provided using hexadecimal format in reversed reciprocal notation where $g_0 = 1$ is dropped. For example, 'A26E7836' in the fourth row of Table I represents $g(x) = x^{32}+x^{30}+x^{26}+x^{23}+x^{22}+x^{20}+x^{19}+x^{18}+x^{15}+x^{14}+x^{13}+x^{12}+x^6+x^5+x^3+x^2+1$. It can be seen from Table I that all the optimum codes have a redundancy r that is at least five less than r_{C}, and have a b that is three more than b_{C}, as guaranteed by the Campopiano bound. The result for $b = 10$ was obtained with 16 parallel threads running on two 3.4 GHz 4-core CPUs for four days.

TABLE I
OPTIMUM SHORTENED CYCLIC CODES FOR $r = 32$.

b	$n_{\max}$	$g(x)$	r_{RA}	r_{C}	b_{RA}	b_{C}
16	108	876CD606	32	37	16	13
15	428	928C9BA5	30	37	16	12
14	1938	C68B3005	28	37	16	11
13	8103	A26E7836	26	37	16	10
12	36505	C39BEE63	27	38	16	9
11	152915	A060FBB9	28	38	15	8
10	596834	A0695362	29	38	13	7

In IEEE 802.3ap, specifically in 10GBASE-KR, an optional $[2112, 2080]$ shortened Fire code, which provides a $2-2.5\,\mathrm{dB}$ gain in signal-to-noise ratio, is used in conjunction with a rate-$64/65$ line code while only a rate-$64/66$ line code is used in the absence of the shortened Fire code, i.e., the total code rate is the same in both cases to simplify the implementation [25], [26]. A primitive $[42987, 42955]$ Fire code with designed burst-error correction capability $b^* = 11$ and $g(x) = (x^{2b^*-1}+1)p(x)$, where $p(x) = (x^{11}+x^2+1)$ is a primitive polynomial of degree $m = 11$, has been used to obtain the $[2112, 2080]$ shortened Fire code in Ethernet. It has been shown that the true burst-error correction capability of a Fire code b can exceed twice their designed burst-error correction capability b^* [5]. However, as $\gcd(2b^*-1, 2^m-1) = 1$ and $b^* \geq 2$, Theorem 3 in [5] can be applied to show that $b = b^*$ for the $[42987, 42955]$ Fire code.

We now evaluate the true burst-error correction capability b of the aforementioned $[2112, 2080]$ shortened Fire code. Table II lists the results of a computer search to find $n_{\max}$ for $11 \leq b \leq 16$ and $g(x) = x^{32}+x^{23}+x^{21}+x^{11}+x^2+1$. Clearly, the shortened Fire code in Ethernet has $b = 11$.

TABLE II
TRUE BURST-ERROR CORRECTION CAPABILITY OF SHORTENED FIRE CODES WITH $g(x) = (x^{21}+1)(x^{11}+x^2+1)$.

b	$n_{\max}$	r_{RA}	r_{C}	b_{RA}	b_{C}
16	33	32	32	16	16
15	33	30	31	16	16
14	33	28	29	16	16
13	33	26	28	16	16
12	114	24	29	16	13
11	42987	26	36	16	9

The question that arises at this point is whether a shortened cyclic code with $r = 32$, $n \geq 2112$, and $b > 11$ exists. Table I shows that such a code, e.g. with $b = 13$ and $n_{\max} = 8103$ exists. Its generator polynomial 'A26E7836' has 17 non-zero coefficients, whereas the generator polynomial of the $[2112, 2080]$ shortened Fire code has six. Therefore, an additional search was performed to identify a shortened cyclic code for $r = 32$, $n \geq 2112$, $b = 13$, and $g(x)$ with a minimum number of non-zero coefficients. The resulting optimum generator polynomial is given by $g(x) = x^{32}+x^{13}+x^8+1$, with $n_{\max} = 2238$. Thus we have shown that a $[2112, 2080]$ shortened cyclic code having $b = 13$ and $g(x)$ with only four non-zero coefficients can be constructed.

IV. Double Burst-Error Detection

Shortened cyclic codes have been widely used to detect errors in codewords with variable length n. These codes, which are typically called CRC codes, have often been designed by means of a generator polynomial of the form $g(x) = p(x)$ or $g(x) = (1+x)p(x)$, where $p(x)$ is a primitive polynomial. If a CRC code has a burst-error correction capability b, then it can also detect any two error bursts of length up to b in a codeword. Next, we compare the double burst-error detection properties of three $r = 32$ CRC codes known as CRC-32, CRC-32C, and CRC-32Q.

The CRC-32 code [27], which is used in Ethernet, SATA, MPEG-2, PKZIP, Gzip, etc., has a primitive generator polynomial in reversed reciprocal notation '82608EDB'. Therefore, it is a cyclic Hamming code for $n = 2^{32}-1$ with minimum distance $d_{\min} = 3$. By means of the Kasami algorithm, we first computed the double burst-error detection capability b as a function of the codeword length n, as depicted in Fig. 1. The maximum codeword lengths corresponding to specific values of b in the range $1 \leq b \leq 16$ are marked by circles. Furthermore, Fig. 1 illustrates the three bounds b_{R}, b_{A} and b_{C} by Reiger, Abramson and Campopiano, respectively, determined by $r = 32$, b and n, where n has been computed as a function of b and $g(x)$ of CRC-32.

For CRC-32, Fig. 2 shows the bounds on r by Reiger (1), Abramson (2) and Campopiano (5) as a function of the codeword length n, computed in the same way as in Fig. 1.

The CRC-32C code [28], which is used in iSCSI, Btrfs, ext4, Ceph, etc., has a generator polynomial in reversed reciprocal notation '8F6E37A0'. Since the generator polynomial is of the form $g(x) = (1+x)p(x)$, it is an extended cyclic Hamming code for $n = 2^{31}-1$ with minimum distance $d_{\min} = 4$. By means of the Kasami algorithm, we first computed the double burst-error detection capability b as a function of the codeword length n, as depicted in Fig. 3. The maximum codeword lengths corresponding to specific values of b in the range $1 \leq b \leq 16$ are marked by circles. Furthermore, Fig. 3 illustrates the three bounds b_{R}, b_{A} and b_{C} by Reiger, Abramson and Campopiano, respectively, determined by $r = 32$, b and n, where n has been computed as a function of b and $g(x)$ of CRC-32C.

For CRC-32C, Fig. 4 shows the bounds on r by Reiger, Abramson and Campopiano as a function of the codeword length n, computed in the same way as in Fig. 3.

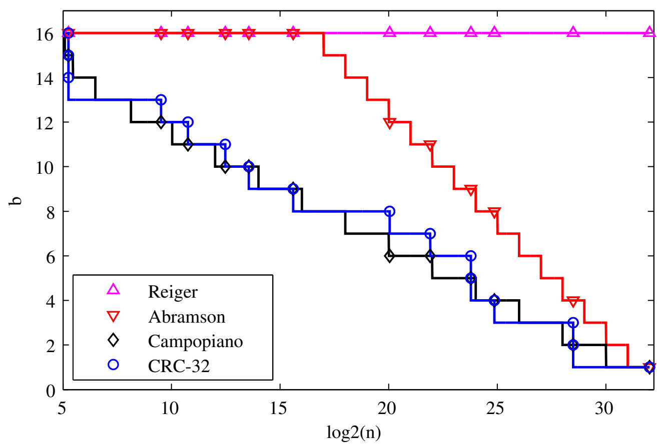

Fig. 1. Error-burst length b as a function of length n for CRC-32.

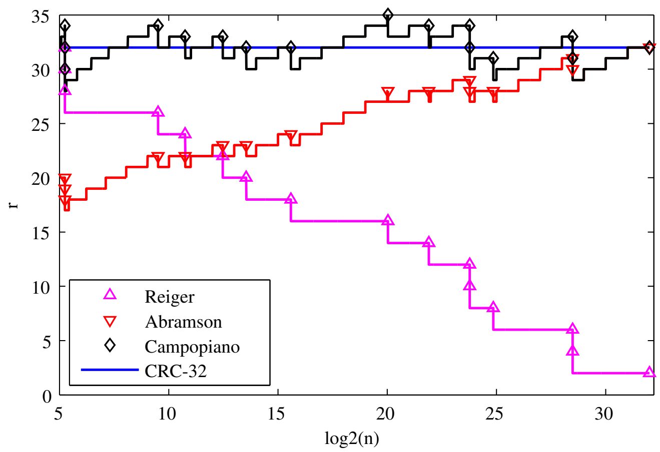

Fig. 2. Redundancy r as a function of length n for CRC-32.

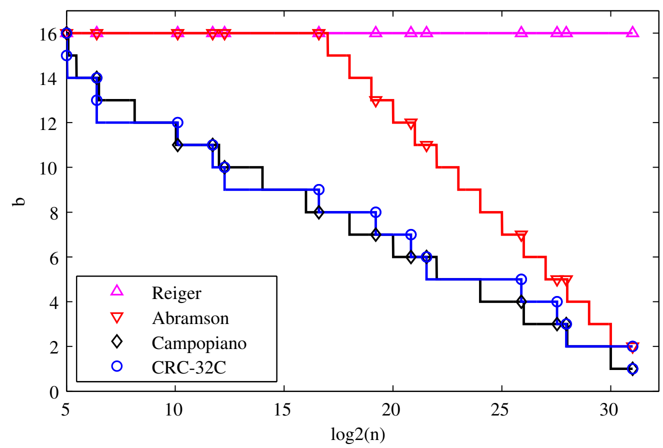

Fig. 3. Error-burst length b as a function of length n for CRC-32C.

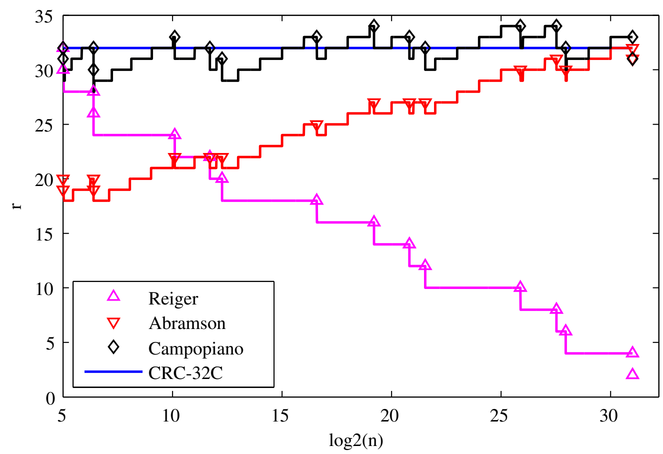

Fig. 4. Redundancy r as a function of length n for CRC-32C.

The CRC-32Q code [29], used in the Aeronautical Information Exchange Model, has a generator polynomial in reversed reciprocal notation 'C0A0A0D5' and is also an extended cyclic Hamming code for $n = 2^{31} - 1$ with minimum distance $d_{\min} = 4$. The double burst-error detection properties of CRC-32Q and corresponding bounds by Reiger, Abramson and Campopiano are depicted in Fig. 5 and Fig. 6 as a function of the codeword length n. Note that for all three CRC codes considered the Abramson bound becomes significantly tighter than the Reiger bound as n increases and b decreases.

Table III compares the double burst-error detection capability of the three CRC codes discussed above. For jumbo frames of size $n \le 72144$ used in Ethernet, CRC-32 has double burst-error detection capability $b = 8$ [16]. Note that CRC-32C and CRC-32Q would achieve $b = 9$ for Ethernet jumbo frames. A maximum double burst-error detection capability of $b = 11$ in jumbo frames with $r = 32$ can be achieved, for example, by the CRC code with generator polynomial 'A060FBB9' in Table I.

V. Conclusion

New optimum binary shortened cyclic codes with redundancy $r = 32$, codeword length $n \le 596834$, and single burst-error correction capability b in the range $10 \le b \le 16$ have been given. The codes have been found by means of the Kasami algorithm in an exhaustive computer search. Their performance has been compared with the Reiger, the Abramson and the Campopiano bounds on the redundancy r and the single burst-error correction capability b depending on the codeword length n.

The true burst-error correction capability of the $[2112, 2080]$ shortened Fire code selected for transmission at $10\,\mathrm{Gb/s}$ in Ethernet has been determined to be $b = 11$. Shortened cyclic codes with higher burst-error correction capability $b = 13$, $r = 32$, and $n \ge 2112$ have been given. A new $[2112, 2080]$ shortened cyclic code with $b = 13$ and a generator polynomial $g(x) = x^{32} + x^{13} + x^8 + 1$ has been presented. This code improves upon the shortened Fire code in Ethernet that has $b = 11$ and six non-zero generator polynomial coefficients.

The double burst-error detection properties of three cyclic redundancy check codes CRC-32, CRC-32C and CRC-32Q used in standards have been analyzed and compared to each other using bounds by Reiger, Abramson and Campopiano. In all three cases, the Abramson bound becomes significantly tighter than the Reiger bound as n increases and b decreases. Finally, double burst-error detection properties should be considered in the selection of a CRC code.

Acknowledgment

The authors would like to thank Prof. Toru Fujiwara for discussions on the Kasami algorithm.

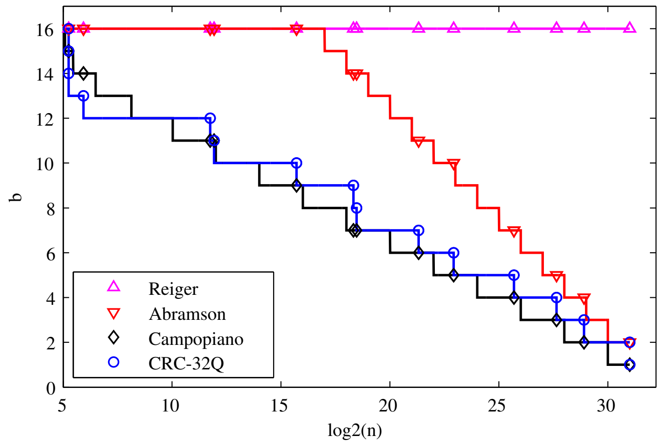

Fig. 5. Error-burst length b as a function of length n for CRC-32Q.

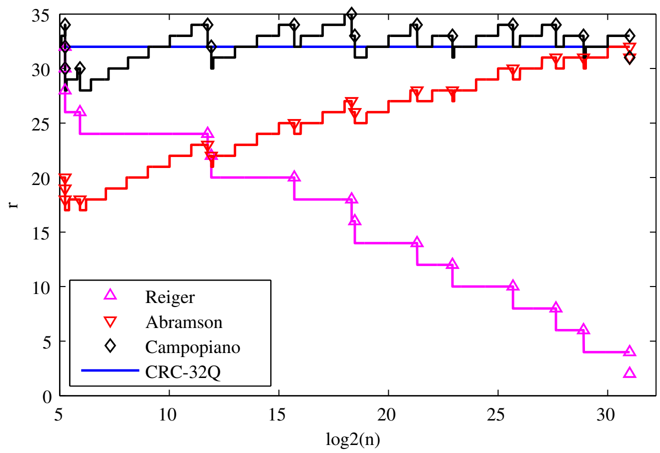

Fig. 6. Redundancy r as a function of length n for CRC-32Q.

TABLE III
COMPARISON OF CRC CODES WITH $r = 32$.

b	CRC-32 $n_{\max}$ [15], [16]	CRC-32C $n_{\max}$	CRC-32Q $n_{\max}$
16	38	32	38
15	38	32	38
14	38	84	38
13	730	84	61
12	1729	1102	3438
11	5680	3354	3880
10	11993	4911	53564
9	49614	98655	326838
8	1077947	603130	362705
7	3932613	1847226	2600285
6	14373575	3040386	7909978
5	14373575	62023779	53935246
4	30435038	193439310	209388432
3	376820508	258958119	502036823
2	376820508	$2^{31}-1$	$2^{31}-1$
1	$2^{32}-1$	$2^{31}-1$	$2^{31}-1$

REFERENCES

[1] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA, USA: MIT Press, 1972.

[2] S. Lin and D. J. Costello, Jr., *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

[3] P. Fire, “A class of multiple-error-correcting binary codes for non-independent errors,” Reconnaissance Syst. Lab., Mountain View, CA, USA, Sylvania Rep. RSL-E-1, Mar. 1959.

[4] H. Matt and J. Massey, “Determining the burst-correcting limit of cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 289–297, May 1980.

[5] W. Zhou, S. Lin, and K. A. S. Abdel-Ghaffar, “On the maximum true burst-correcting capability of Fire codes,” *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5323–5342, Oct. 2016.

[6] T. Kasami, “Optimum shortened cyclic codes for burst-error correction,” *IEEE Trans. Inf. Theory*, vol. 9, no. 2, pp. 105–109, Apr. 1963.

[7] S. H. Reiger, “Codes for the correction of ’clustered’ errors,” *IRE Trans. Inf. Theory*, vol. 6, no. 1, pp. 16–21, Mar. 1960.

[8] N. M. Abramson, “Error-correcting codes from linear sequential circuits,” presented at the 4th Symp. Inf. Theory, London, U.K., Aug. 29-Sep. 2, 1960.

[9] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2002.

[10] C. N. Campopiano, “Bounds on burst error correcting codes,” Radio Corporation of America, Airborne Systems Division, EM-60-597-20, Jan. 1961.

[11] ——, “Bounds on burst-error-correcting codes,” *IRE Trans. Inf. Theory*, vol. 8, no. 3, pp. 257–259, Apr. 1962.

[12] W. H. Kautz and K. N. Levitt, “A survey of progress in coding theory in the Soviet union,” *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 197–244, Jan. 1969.

[13] S. Jain, “Campopiano-type bounds in non-Hamming array coding,” *Linear Algebra and its Applications*, vol. 420, no. 1, pp. 135 – 159, 2007.

[14] “IEEE Standard for Ethernet,” *IEEE Std 802.3-2015*, pp. 1–4017, Mar. 2016.

[15] T. Fujiwara, T. Kasami, and S. Lin, “Error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE Standard 802.3,” *IEEE Trans. Commun.*, vol. 37, no. 9, pp. 986–989, Sep. 1989.

[16] R. D. Cideciyan and M. Gustlin, “Double burst error detection capability of Ethernet CRC,” Jul. 2012, IEEE 802.3bj Task Force Meeting. [Online]. Available: http://www.ieee802.org/3/bj/public/jul12/cideciyan_01_0712.pdf

[17] L. J. Garcia Villalba, J. R. Fuentes Cortez, and M. Blaum, “On the efficiency of shortened cyclic single-burst-correcting codes,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3290–3296, Jul. 2010.

[18] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[19] H. D. L. Hollmann and L. M. G. M. Tolhuizen, “Optimal codes for correcting a single (wrap-around) burst of erasures,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4361–4364, Sep. 2008.

[20] B. Sharma and B. Dass, “Extended Varshamov-Gilbert and sphere-packing bounds for burst-correcting codes,” *IEEE Trans. Inf. Theory*, vol. 20, no. 2, pp. 291–292, Mar. 1974.

[21] K. Abdel-Ghaffar, R. McEliece, A. Odlyzko, and H. van Tilborg, “On the existence of optimum cyclic burst-correcting codes,” *IEEE Trans. Inf. Theory*, vol. 32, no. 6, pp. 768–775, Nov. 1986.

[22] J. Massey, “Shift-register synthesis and BCH decoding,” *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[23] A. Dür, “A fast algorithm to determine the burst-correcting limit of cyclic or shortened cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 504–509, Mar. 1992.

[24] L. J. Garcia Villalba, J. R. Fuentes Cortez, A. L. Sandoval Orozco, and M. Blaum, “An efficient algorithm for searching optimal shortened cyclic single-burst-correcting codes,” *IEEE Commun. Lett.*, vol. 16, no. 1, pp. 89–91, Jan. 2012.

[25] A. Belegolovy *et al.*, “Update on FEC proposal for 10GbE backplane Ethernet,” Nov. 2005, IEEE 802.3ap Task Force Meeting. [Online]. Available: http://ieee802.org/3/ap/public/nov05/ganga_02_1105.pdf

[26] A. Szczepanek, I. Ganga, C. Liu, and M. Valliappan, “10GBASE-KR FEC tutorial,” Jul. 2006, IEEE 802 Plenary. [Online]. Available: http://www.ieee802.org/802_tutorials/06-July/10GBASE-KR_FEC_Tutorial_1407.pdf

[27] J. L. Hammond, J. E. Brown, and S. S. Liu, “Development of a transmission error model and an error-control model,” Tech. Rep., Rome Air Develop. Cen., RADC-TR-75-138, May 1975.

[28] G. Castagnoli, S. Bräuer, and M. Herrmann, “Optimization of cyclic redundancy-check codes with 24 and 32 parity bits,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 883–892, Jun. 1993.

[29] J. K. Wolf and D. Chun, “The single burst error detection performance of binary cyclic codes,” *IEEE Trans. Commun.*, vol. 42, no. 1, pp. 11–13, Jan. 1994.