On the binary CRC codes used in the HARQ scheme of the LTE standard

Peter Kazakov

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

September, 2013
Albena, Bulgaria

Introduction I

- We investigate CRC codes generated by polynomials of degree $r = 24$ and minimum distance 4.
- Order of polynomial $g(x)$ is number n_c, such that $g(x)$ divides $x^{n_c} + 1$ and $n_c = min\{m | x^m \equiv 1 \; mod \; g(x)\}$
- Probability of undetected error can be expressed in the following way

$$P_{ud}(C, \varepsilon) = \sum_{i=1}^{n_c} A_i \varepsilon^i (1 - \varepsilon)^{n-i}$$

- Denote the number of minimum weight codewords by $A_{d,n_c - s}(g)$ for a shortened in s positions $[n_c - s, k_c - s, d = 4]$ CRC code.

Introduction II

- Historically, standardized polynomials of degree r were chosen with a parity control check polynomial of the type $(x + 1)$ multiplied by a primitive polynomial of degree $r - 1$.

Introduction III

- Castagnoli, Brauer, Herrman, CRC 8, CRC 16
- Fujiwara, Kasami and all, 1985, CRC 16
- T. Baicheva, S. Dodunekov and P. Kazakov, On the cyclic redundancy-check codes with 8 bit redundancy, Computer Communications, v. 21, 1998
- T. Baicheva, S. Dodunekov and P. Kazakov, Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy, IEE Proc. Comm., 2000
- P. Kazakov, Fast Calculation of the Number of Minimum-weight Words of CRC Codes, IEEE Trans. On Inf.Theory, volume 47, 2001.
- CRC-24 standards FlexRay(0x15D6DCB), OpenPGP(0x1864CFB)
- CRC 32 - Castagnoli 93, arbitrary polynomials

Introduction IV

- CRC32 - Koopman (exhaustive search, 30 Alpha stations for 3-4 months)

Introduction V

Criterias:

- max (d=4), min(weight(g(x))
- Criterias good and proper, Dodunekov and Dodunekova
- max (N), such that d=6 for CRC codes up to length N, d=4 for the rest
- $max(d), min(A_d)$

Problem complexity (for given codelength n):

- We need to investigate all polynomials 2^r, such that $ord(g) > n$
- We need to use Gray code to generate dual distance distribution (2^r)
- We need to calculate weight of each line (n_c)
- We need to apply MacWillians transformation to obtain d and A_d

LTE standard and CRC codes I

- Next commercial standard after CDMA, WCDMA and TDSCDMA
- 4G, first commercial release available 2009
- Supports scalable carrier bandwidths, from 1.4 MHz to 20 MHz
- Target downlink 1Gbs static and 100Mbs car, uplink 50 Mbit/s
- Support both TDD and FDD, based on HSPDA, which includes:
- Hybrid automatic repeat-request (HARQ), minor errors can be corrected without retransmission
- Adaptive modulation (good radio conditions 16QAM and 64QAM) and coding
- MIMO

LTE standard and CRC codes II

CRC attachment -> Turbo coding -> Bit scrambling -> HARQ rate matching -> Interleaving and interlacing

- Rate matching with puncturing: fast way to calculate BER
- CRC encoding and decoding
- Turbo codes used: 1/3
- Bit scrambling: suffficiently random sequence
- Transport Block (TB) -> >100000 bits, encoded with g_a
- Each TB contains of code blocks (Cbs) with lenght 6120, encoded with g_b
- Early detection scheme: minimum number of iteration before decoder is stopped, retransmission on CRC error

LTE standard and CRC codes III

- $g_{24A}(x) = x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ and;
- $g_{24B}(x) = x^{24} + x^{23} + x^6 + x^5 + x + 1$ for a CRC length L = 24 and
- $g_{16}(D) = x^{16} + x^{12} + x^5 + 1$ for a CRC length L = 16.
- $g_8(D) = x^8 + x^7 + x^4 + x^3 + x + 1$

Method of investigation I

Theorem 1

Let C be a binary $[n_c - r, k_c, 4]$ *code generated by the polynomial* $(x+1)g(x)$ *of degree r and order* $n_c = 2^{r-1} - 1$*. The following equality holds:*

$$A_{4,n_c-s}(g) = \frac{(n_c-3)((n_c-4s)(n_c-1)+6s(s-1))}{24} -$$

$$\sum_{m=2}^{max(2,s-1)} \sum_{j=1}^{m-1} (s-m)(Q_{m,j}(g) - \sum_{l=1}^{j-1} Q_{m,j,l}(g))$$

Method of investigation II

$$Q_{m,j}(g) = \begin{cases} 1, & g(x) \mid x^m + x^j + 1, \\ 0, & \text{otherwise} \end{cases}$$

$$Q_{m,i,j}(g) = \begin{cases} 1, & g(x) \mid x^m + x^j + x^i + 1, \\ 0, & \text{otherwise.} \end{cases}$$

Method of investigation III

Definition 2

If two polynomials g(x) and f(x) can be factorized on an equal number k of irreducible polynomials $g_1(x), \ldots, g_k(x)$ and $f_1(x), \ldots, f_k(x)$ such that $deg(g_i(x)) = deg(f_i(x))$ for $i = 1, \ldots, k$ and $ord(g_i(x)) = ord(f_i(x))$ for $i = 1, \ldots, k$ we will say that they belong to one class.

- We group all polynomials in classes, we exclude reciprocal ones;
- For each class, we select one polynomial h and we calculate the minimum distance d of the corresponding CRC code. If $d = 3$, we skip this class;

Method of investigation IV

- For each class represented by a polynomial h, we calculate the number of minimum weight codewords $A_{4,6120}(h)$ and select two groups of polynomial classes - one with a polynomial representative of order bigger than 6120 and one of order bigger than $100,000$.
- For the first m classes with a minimum value of $A_{d=4,6120}$ and the first three classes with a minimum value of $A_{d=4,100,000}$ and an order bigger than $100,000$ (in order to compare with g_B) and big codelengths we perform calculations on all their members. In that way we find the best polynomial from the corresponding class that generates a minimum $A_{d=4,6120}$.

Results I

Order > 6120

Polynomial notation	*order*	$A_{d,6120}$
0x1864CFB (standard,g_A)	$2^{23}-1$	56,416,496
0x114855B	38227	24,989,800
0x17A481F	12291	25,013,640
0x14AC147	19065	25,463,304

Order > 100,000

Polynomial notation	*order*	$A_{d,6120}$
0x1800063 (standard,g_B)	$2^{23}-1$	68,018,112
0x103A977	114681	25,201,272
0x116C3EF	522753	25,850,512
0x140F133	278845	29,275,776

Results II

It is worth investigating following class candidates:

- $(x^3 + x^2 + 1)(x^7 + x^6 + 1)$.IrrPol
- $(x^4 + x + 1)$.IrrPol

This study is an enablement for CRC-32 case. Still few steps have to be done:

- Get analytical formula for the two cases above.
- Map all calculations on a GPU
- Get early bailout criterias [Koopman]