3GPP TSG RAN1 #51 R1-075016
Jeju, Korea
November 5 - 9, 2007

Agenda Item:	**6.3**
Source:	**Broadcom**
Title:	**One CRC polynomial is sufficient for both CB and TB CRC**
Document for:	**Discussion and Decision**

1. Summary

Two layers CRC (cyclic redundancy check), one for turbo code blocks (CB) and the other for transport block (TB) is adopted in TS 36.212 [1]. At RAN1 Shanghai meeting, two different CRC generator polynomials [2] are "agreed as working assumption, to be revisited if it is found that second polynomial is not needed". This document shows that indeed the second polynomial *is not necessary*, i.e. one CRC polynomial is sufficient for two layers CRC.

There are two possible ways to judge a CRC system, namely,

1) Statistic method (relate to specific channel), which computes the probability of *undetectable error* based on the given channel. Due to the complexity of mobile radio channel, so far there is no clear way to use this method in mobile channel.

2) Combinatorial method (not relate to channel), which computes the number of all possible error vectors that are undetectable by the CRC. Usually this method gives an upper bound of the probability of undetectable error.

In this document, we use the combinatorial method.

The following two different two layers CRC systems are considered in this document,

- *Equal-polynomial-system:* Both CB and TB use the same CRC generator polynomial
- *Unequal-polynomials-system*: CB and TB use different CRC generator polynomial, respectively.

In [3], a special case of TB with two CBs is considered, which satisfies the following three conditions:

a) One CB is correctly decoded;
b) The other CB has undetectable error; and
c) Error in TB is undetectable.

The first part of this document contributes to this special case. We calculate the number of error vectors that satisfy a),b) and c) for both Equal-polynomial-system and Unequal-polynomial-system. It turns out that they are the same. In the second part of this document we prove the same conclusion in general, i.e. without the restrictions a),b) and c). With this conclusion, we can say that one CRC polynomial is sufficient for both CB and TB CRC.

2. Polynomial representation of binary vectors and notation on two layers CRC

Following the convention in information theory we represent a binary vector of size n, $x_0, x_1, \ldots . x_{n-1}$ by a polynomial $X(D)$ of degree n-1, namely

$$(x_0, x_1, \ldots, x_{n-1}) \leftrightarrow X(D) = x_{n-1}D^{n-1} + x_{n-2}D^{n-2} + \cdots x_1 D + x_0$$

In this document we denote L the size of CRC redundancy, $G_{TB}(D)$ the CRC generator polynomial for TB, and $G_{CB}(D)$ the CRC generator polynomial for CB. Denote *i*-th CB by CB(*i*) and its size by k_i. In this document, we only consider the case that one TB has *N>1* CBs, see Fig.1. In fact, when N=1 TB CRC is CB CRC.

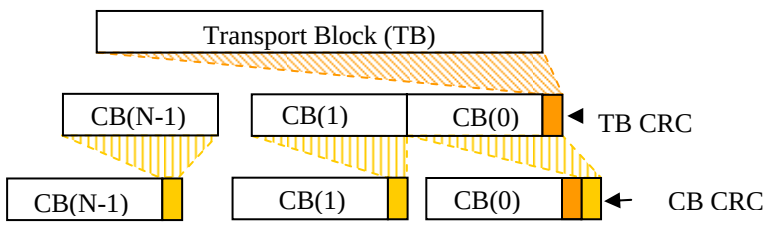

Figure 1 Tow layers CRC

An information stream in CB(*i*) can be represent by a binary polynomial $I(D)$ of degree less than k_i and the codeword after CRC encoding is $I(D)D^L + CRC_{CB,i}(D)$ such that $\deg CRC_{CB,i}(D) < L$ and $I(D)D^L + CRC_{CB,i}(D) = G_{CB}(D)Q(D)$ for some polynomial $Q(D)$.

3. Special case: Undetectable error on one code block

Consider a TB of two code blocks. In this section we study a special case that satisfies the following 3 conditions:

a) One code block, say CB(0), is correctly decoded;
b) The errors in the other code block, say CB(1), is undetectable; and
c) The errors in TB is also undetectable.

This special case has been considered in [3]. However, the conclusion given by the following proposition is different to that in [3].

Proposition

$$\begin{aligned} &\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) = G_{CB}(D)\} \\ =&\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) \neq G_{CB}(D)\} \\ =&\#\{V(D) \neq 0 \mid \deg V(D) < k_1 - L\} = 2^{k_1 - L} - 1 \end{aligned}$$

Proof : See Appendix I.

4. General: Number of all possible undetectable error vectors

Let $X_i(D), i = 0,\ldots,N-1$ be N systematic vectors (polynomials) for N code blocks CB(i), $i = 0,1,\ldots,N-1$. Then $\deg X_i(D) < k_i$. Let $CRC_{TB}(D)$ be the CRC redundancy of TB, then

$$\left\| \left[\sum_{i=1}^{N-1} X_i(D) D^{\left\{L+\sum_{j=0}^{i-1} k_j\right\}} + X_0(D)D^L + CRC_{TB}(D) \right] = G_{TB}(D)H(D) \qquad \text{(EQ-2)}$$

Let $CRC_i(D)$ be CRC redundancy of CB(i). Then

$$X_i(D)D^L + CRC_i(D) = G_{CB}(D)Q_i(D), \mathrm{i} = 0,\ldots,\mathrm{N-1}$$

An error vector on a TB after turbo decoding can be represented by a polynomial $E(D)$ of degree at most $\sum_{i=1}^{N-1}(k_i + L) + (k_0 + 2L) - 1$. This error polynomial can be decompose into

$$E(D) = E_{N-1}(D)D^{k_0+\cdots k_{N-2}+NL} + \cdots + E_2(D)D^{k_0+k_1+3L} + E_1(D)D^{k_0+2L} + E_0(D) \qquad \text{(EQ-3)}$$

where $\deg(E_0(D)) < k_0 + 2L$ and $\deg(E_i(D)) < k_i + L$ for $i = 1,\ldots,N-1$. Moreover, we denote

$$E_i(D) = E_{i,1}(D)D^L + E_{i,2}(D),\ i = 0,1,\cdots,N\text{-}1$$

such that $\deg E_{0,1}(D) < k_0 + L$ and $\deg E_{i,1}(D) < k_i$ for $i > 0$, and $\deg E_{i,2}(D) < L$ for $i \geq 0$. If the error vector $E(D)$ is undetected by two layered CRC, then

$$E_{i,1}(D)D^L + E_{i,2}(D) = G_{CB}(D)V_i(D), i = 0,\ldots,N-1 \text{ and}$$

$$E_{N-1,1}(D)D^{k_0+\cdots k_{N-2}+L} + \cdots + E_{2,1}(D)D^{k_0+k_1+L} + E_{1,1}(D)D^{k_0+L} + E_{0,1}(D) = G_{TB}(D)W(D) \qquad \text{(EQ-4)}$$

Theorem

$$\begin{aligned} &\#\{\text{Error vectors undetectable by two layered CRC} \mid G_{TB}(D) = G_{CB}(D)\} \\ &= \#\{\text{Error vectors undetectable by two layered CRC} \mid G_{TB}(D) \neq G_{CB}(D)\} \\ &= \#\{U(D) \neq 0 \mid \deg U(D) < \sum_{i=0}^{N-1} k_i\} = 2^{\sum_{i=1}^{N} k_i} - 1 \end{aligned}$$

Sketch of the proof: Without using the condition of either $G_{CB}(D) = G_{TB}(D)$ or $G_{CB}(D) \neq G_{TB}(D)$, we prove the following two facts.

Fact 1: For any given error vector $E(D)$ undetectable by two layered CRC, there exist a polynomial $U(D)$ of degree less than $\sum_{i=0}^{N-1} k_i$ such that $E(D)$ is uniquely determined by $U(D)$.

Fact 2: Given any polynomial $U(D)$ of degree less than $\sum_{i=0}^{N-1} k_i$ an error vector $E(D)$ that will be undetected by two layered CRC can be constructed.

See Appendix II for detailed proof.

5. Conclusion

It is proved that the number of possible error events that undetectable by two layered CRC does not depend on whether $G_{CB}(D) = G_{TB}(D)$ or $G_{CB}(D) \neq G_{TB}(D)$. Therefore, we suggest using one generator polynomial for both CB and TB CRC.

6. References

[1] 3GPP TS 36.212 v8, "Multiplexing and Channel Coding (Release 8)," 2007.

[2] 3GPP R1-074015, "TB CRC generator polynomial," Ericsson, ITRI, LGE, Motorola, Nokia, Nokia Siemens Networks, Nortel, Qualcomm, Samsung

[3] 3GPP R1-074492, "Details on Probabilities of Undetected TB Errors." Ericsson

7. Appendix I: Proof of Proposition

To prove the proposition we need the following well known lemma.

Lemma 1 Let $G(D)$ be a binary polynomial. Then for any given binary polynomial $Y(D)$ there exist two unique polynomials $Q(D)$ and $r(D)$ such that

$$X(D) = G(D)Q(D) + r(D) \text{ with } \deg r(D) < \deg G(D).$$

Proof of Proposition Let $E'(D)$ be an error vector that satisfy Conditions a)-c). By Condition a) it must be in CB(1). Thus $E'(D) = E(D)D^{k_0+2L}$ with $\deg E(D) \le k_1 + L$. Condition b) tells that this error vector cannot be detected by CB(1) CRC. Thus, $E(D) = G_{CB}(D)H(D)$ with $\deg H(D) \le k_1$. Let us denote $E(D) = E_1(D)D^L + E_2(D)$ with $\deg E_1(D) \le k_2$ and $\deg E_2(D) < L$. Condition c) implies that $E_1(D)$ cannot be detected by TB CRC, i.e. $E_1(D) = G_{TB}(D)V(D)$ with $\deg V(D) < k_2 - L$.

Equal Case ($G_{TB}(D) = G_{CB}(D)$): In this case we have $E_1(D) = G_{CB}(D)V(D)$ .Thus $G_{CB}(D)V(D)D^L + E_2(D) = G_{CB}(D)H(D)$ .This implies $E_2(D) = 0$ since $\deg E_2(D) < L$. Thus

$$E(D) = E_1(D)D^L = G_{CB}(D)V(D)D^L .$$

This implies that $E(D)$ is determined by polynomial $V(D)$ of degree less than $k_1 - L$. Therefore

$$\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) = G_{CB}(D)\} \le \#\{V(D) \ne 0 \mid \deg V(D) < k_1 - L\} \quad \text{(EQ-5)}$$

On the other hand, for any polynomial $V(D)$ of degree less than $k_1 - L$, take

$$E(D) = G_{CB}(D)V(D)D^L = G_{TB}(D)V(D)D^L . \quad \text{(EQ-6)}$$

Take error vector $E'(D) = E(D)D^{k_0+2L}$ as an error vector. This error vector satisfies Condition a). (EQ-6) implies that $E(D)$ cannot be detected by CB CRC, i.e. satisfy Condition b) is satisfied. Since the minimal term degree of $E(D)$ is at least L this error vector will passed to TB. Then by (EQ-6) again $E'(D) = E(D)D^{k_0+2L}$ cannot be detected by TB CRC, i.e. it satisfies Condition c). Therefore

$$\#\{\text{Error vectors satisfying 1), 2) and 3)} \mid G_{TB}(D) = G_{CB}(D)\} \ge \#\{V(D) \ne 0 \mid \deg V(D) < k_1 - L\} \quad \text{(EQ-7)}$$

Combining (EQ-5) and (EQ-7), we have

$$\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) = G_{CB}(D)\} = \#\{V(D) \ne 0 \mid \deg V(D) < k_1 - L\}$$
$$= 2^{k_1 - L} - 1$$

Unequal Case ($G_{CB}(D) \ne G_{TB}(D)$): By Condition c) $E_1(D) = G_{TB}(D)V(D)$.
Thus $E(D) = G_{CB}(D)H(D) = G_{TB}(D)V(D)D^L + E_2(D)$ with $\deg E_2(D) < L = \deg G_{CB}(D)$. By Lemma 1, $E_2(D)$ and $H(D)$ are uniquely determined by $V(D)$. Therefore, $E(D)$ is also determined by $V(D)$. Thus

$$\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) \ne G_{CB}(D)\} \le \#\{V(D) \ne 0 \mid \deg V(D) < k_1 - L\} \quad \text{(EQ-8)}$$

On the other hand, for any polynomial $V(D)$ of degree less than $k_2 - L$, by Lemma 1 there always exist tow unique polynomials $H(D)$ and $E_2(D)$ such that

$$G_{TB}(D)V(D)D^L = G_{CB}(D)H(D) + E_2(D) \text{ with } \deg E_2(D) < L .$$

Denote $E(D) = G_{CB}(D)H(D)$ and take error vector $E'(D) = E(D)D^{k_0+2L}$. Then this error vector satisfies Condition a) and it cannot be detected by CB CRC, i.e. satisfy Condition b). Since $E(D) - E_2(D) = G_{TB}(D)V(D)D^L$, the error vector pass to TB is $G_{TB}(D)V(D)D^{L+k_1}$ which cannot be detected by TB CRC, i.e. Condition c) is satisfied. Therefore

$$\#\{\text{Error vectors satisfying a), b) and c)} \mid G_{TB}(D) \neq G_{CB}(D)\} \geq \#\{V(D) \neq 0 \mid \deg V(D) < k_1 - L\} \qquad \text{(EQ-9)}$$

Combining (EQ-8) and (EQ-9), we have

$$\begin{aligned}&\#\{\text{Error vectors satisfing a), b) and c)} \mid G_{TB}(D) \neq G_{CB}(D)\} = \#\{V(D) \neq 0 \mid \deg V(D) < k_1 - L\}\\ &= 2^{k_1 - L} - 1\end{aligned}$$

We have shown that the numbers of possible error vectors in two cases are the same. This proves the proposition.

8. Appendix II: Proof of Theorem

The following well known lemma will be used in the proof.

Lemma 2 Let $G(D)$ be a CRC generator polynomial of degree L. Then, given any polynomial $X(D)$ there exist a unique polynomial $C(D)$ of degree less than L such that $X(D)D^L + C(D)$ is a code word of this CRC. i.e. $X(D)D^L + C(D) = G(D)Q(D)$.

Proof of Theorem: Let $E(D)$ be an error vector after turbo decoding (as defined in Section 4) such that it cannot be detected by two layers CRC. Then, the individual error vector in CB(i), namely $E_i(D)$ as defined in (EQ-2) cannot be detected by CB CRC for $i = 0, \ldots, N-1$. This implies that $E_i(D)$ is a CB CRC codeword, i.e.

$$E_i(D) = E_{i,1}(D)D^L + E_{i,2}(D) = G_{CB}(D)Q_i(D)$$

with $\deg E_{i,1}(D) < k_i$ $i > 0$, $\deg E_{0,1}(D) \leq k_0 + L$ and $\deg E_{i,2}(D) < L$, $i \geq 0$. By Lemma 2, we conclude

$$E_{i,2}(D) \text{ is uniquely determined by } E_{i,1}(D). \qquad \text{(EQ-10)}$$

The error vector after CB CRC is $E_{N-1,1}(D)D^{\sum_{i=0}^{N-2} k_i + L} + \cdots + E_{11}(D)D^{k_0+L} + E_{01}(D)$. By the assumption of the theorem, this error cannot be detected by TB CRC. This implies

$$E_{N-1,1}(D)D^{\sum_{i=0}^{N-2} k_i + L} + \cdots + E_{11}(D)D^{k_0+L} + E_{01}(D) = G_{TB}(D)U(D) \qquad \text{(EQ-11)}$$

Thus $(E_0(D), E_1(D), \cdots, E_{N-1,1}(D))$ is determined by polynomial $U(D)$, and so does the error vector $E(D)$ by (EQ-10). Since the degree of the left side of the polynomial in (EQ-11) is at most $\sum_{j=0}^{N-1} k_i + L$, the degree of $G_{TB}(D)U(D)$ is also at most $\sum_{j=0}^{N-1} k_i + L$. Thus the degree of $U(D)$ is at most $\sum_{j=0}^{N-1} k_i$. This proves

$$\#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) = G_{CB}(D)\} \le \#\{U(D) \ne 0 \mid \deg U(D) < \sum_{j=0}^{N-1} k_i\}$$

and

$$\#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) \ne G_{CB}(D)\} \le \#\{U(D) \ne 0 \mid \deg U(D) < \sum_{j=0}^{N-1} k_i\}$$

(EQ-12)

On the other hand, given any polynomial $U(D)$ of degree less than $\sum_{j=0}^{N-1} k_i$. There exist a polynomial vector $(E_0(D), E_1(D), \cdots, E_{N-1,1}(D))$ such that (EQ-11) hold. This shows that the error vector $E_{N-1,1}(D)D^{\sum_{i=0}^{N-2} k_i + L} + \cdots + E_{11}(D)D^{k_0+L} + E_{01}(D)$ cannot be detected by TB CRC. By Lemma 2, for every $E_{i,1}(D)$ there exists a polynomial $E_i(D)$ of degree less than $k_i + L$ for $i > 0$ and $\deg E_0(D) < k_0 + 2L$ such that

$$E_i(D) = E_{i1}(D)D^L + E_{i2}(D) = G_{CB}(D)Q_i(D)$$

This means that the error vector $E_i(D)$ (which may be 0 for some i) cannot be detected by CB CRC. Therefore the error vector

$$E(D) = E_0(D) + E_1(D)D^{k_0+2L} + E_2(D)D^{k_0+k_1+3L} + \cdots + E_{N-1}(D)D^{k_0+\cdots k_{N-2}+NL}$$

determined by $U(D)$ will be undetected by two layers CRC. This proves

$$\#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) = G_{CB}(D)\} \ge \#\{U(D) \ne 0 \mid \deg U(D) < \sum_{j=0}^{N-1} k_i\}$$

and

$$\#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) \ne G_{CB}(D)\} \ge \#\{U(D) \ne 0 \mid \deg U(D) < \sum_{j=0}^{N-1} k_i\}$$

(EQ-13)

With (EQ-12) and (EQ-13), we can conclude

$$\#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) = G_{CB}(D)\}$$
$$= \#\{\text{Error vectors undetectable by two layers CRC} \mid G_{TB}(D) \neq G_{CB}(D)\}$$
$$= \#\{U(D) \neq 0 \mid \deg U(D) < \sum_{j=0}^{N-1} k_i\} = 2^{\sum_{j=0}^{N-1} k_i} - 1$$