Flip CRC Modification for Message Length Detection

Shin-Lin Shieh, Po-Ning Chen, *Senior Member, IEEE*, and Yunghsiang S. Han, *Member, IEEE*

***Abstract*—Cyclic redundancy check (CRC) bits that are conventionally used for error detection have recently found a new application in universal mobile telecommunications system standard for message length detection of variable-length message communications. It was anticipated that the CRC bits, when they are coworked with the inner convolutional code, can be used to detect the receiver—unaware of the message length—without much degradation in their error detection capability. This is unfortunately not true when the offset or difference between the wrong detected length and the true length is small. Two improvements, i.e., the DoCoMo's reverse CRC method and the flip CRC method, were accordingly proposed. In this paper, we revisited the flip CRC modification by considering the impact of joint decoding of the CRC code and the convolutional code. By generalizing the condition for the selection of the flip polynomials, we found that under error-free transmission, the range of the length offsets, at which the false length probability conditioning on the true message length can be made exactly zero (and hence, is minimized), can be extended from $\ell - 1$ to $\ell + m - 1$, where ℓ and m are, respectively, the number of the CRC bits and the memory order of the convolutional code. In addition, an upper bound and a lower bound for the overall false length probability with respect to a uniform pick of the true message length over a candidate message length set are derived. It is then confirmed numerically that the two bounds almost coincide for moderate $(\ell + m)$ value. Simulations show that the false length probability obtained analytically under error-free transmission assumption only mildly degrades for moderate-to-high SNRs. Interestingly, we also found that the system block error rate of the flip CRC method can be well approximated by the performance curve of the adopted convolutional code up to a certain SNR, and approach an error floor determined well by the previously derived false length probability bounds beyond this SNR, thereby facilitating the selection of the system parameters, such as the number of CRC bits and the memory order of the convolutional code.**

***Index Terms*—Blind rate detection, blind transport format detection, cyclic redundancy check (CRC), length detection, variable-length message.**

I. Introduction

IT IS QUITE common in communication systems that the length of transmitted message blocks varies. To help deblocking the messages, block length information is often transmitted either together with the messages or through an explicit control channel. Usually, the integrity of message blocks are protected with an error-detecting code. An error correcting code is then applied to recover channel errors.

The cyclic redundancy check (CRC) code is perhaps the most frequently used error-detecting code. An ℓ-bit CRC code can be specified by its generator polynomial $g_\ell(x)$ that is commonly required to satisfy $g_\ell(x) = (x+1)b(x)$, where $b(x)$ is a primitive polynomial of order $(\ell - 1)$ [2]. The $(x+1)$ factor in the CRC generator polynomial ensures the detectability of all odd-weight error patterns, while a primitive $b(x)$ guarantees that all double errors are detectable as long as the message length is less than $2^{\ell-1}$.

Due to its feasibility, the convolutional code is prevalent in the practice of error correcting coding technique. Conventionally, a convolutional code is denoted by a three tuple (n, υ, m) in which the three parameters indicate its realization of υ-input, n-output linear sequential circuit with input memory m. Since the inputs stay in the encoder for an additional m time units, adding m zeros at the end can retrieve the encoder to the all-zero state. In this paper, we will focus on $(n, 1, m)$ convolutional codes.

In a variable-length-message communication system, the transmission of message length information requires additional system overhead. In some specific applications, the data rate is so low that the transmission of such additional length information may become an inefficient system burden. An example is the adaptive multirate (AMR) mode of universal mobile telecommunications system (UMTS) wideband code-division multiple-access (WCDMA) standard for compressed speech transmission, in which the transmission overhead for message length could be as large as 3 kb/s, which consumes almost 25% of the 12.2 kb/s data rate. In such case, detection of message length through the attached CRC bits with the help of inner convolutional code decoder becomes a potential system alternative. It is conceptually proposed in the *blind transport format detection using CRC* in [12, pp. 56–58] that a length is accepted as a legal candidate when a certain node on the decoding trellis of the convolutional code gives the smallest metric among all nodes at the same trellis time index, and meanwhile, the validity test of the CRC bits is passed (cf., Fig. 1).

The original plan of the *blind transport format detection using CRC* is to specialize a system that the block error rate (BLER) and the undetected error rate (UER) are able to be, respectively, made lower than their corresponding system requirements without the length overhead. To achieve this objective, not only a joint convolutional/CRC decoder is proposed, but also a candidate message length set $\mathcal{K} \triangleq \{k_1, k_2, \ldots, k_p\}$ consisting of all block lengths that is allowed to be used by the transmitter is specified. Intuitively, if the convolutional code decoder corrects all channel errors, the probability that the ℓ-bit CRC validity test

Paper approved by T. -K. Truong, the Editor for Coding and Communication Theory of the IEEE Communications Society. Manuscript received June 23, 2005; revised February 8, 2006. This work was supported in part by the National Science Council of Taiwan, R.O.C., under Grant NSC 94-2213-E-305-001 and Grant NSC 95-2221-E-305-005. This work was presented at the International Symposium on Information Theory and its Applications 2004, Parma, Italy, October 2004.

S. L. Shieh is with the Sunplus mMobile, Inc., Hsinchu 300, Taiwan, R.O.C., and also with the Department of Communications Engineering, National Chiao-Tung University, Hsinchu 300, Taiwan, R.O.C. (e-mail: shinlinshieh@yahoo.com.tw).

P.-N. Chen is with the Department of Communications Engineering, National Chiao-Tung University, Hsinchu 300, Taiwan, R.O.C. (e-mail: qponing@mail.nctu.edu.tw).

Y. S. Han is with the Graduate Institute of Communication Engineering, National Taipei University, Taipei 237, Taiwan, R.O.C. (e-mail: yshan@mail.ntpu.edu.tw).

Digital Object Identifier 10.1109/TCOMM.2007.904392

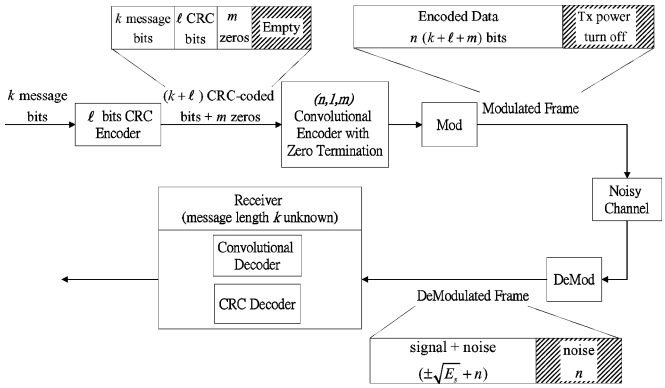

Fig. 1. Block diagram and frame structure of the *blind transport format detection using CRC* proposed in UMTS WCDMA standard. In the system, the receiver only knows the set $\mathcal{K} \triangleq \{k_1, k_2, \ldots, k_p\}$ of message lengths possibly used by the transmitter, but is not aware of the true message length k. The receiver, therefore, has to detect the true message length through the attached CRC bits with the help of convolutional decoder.

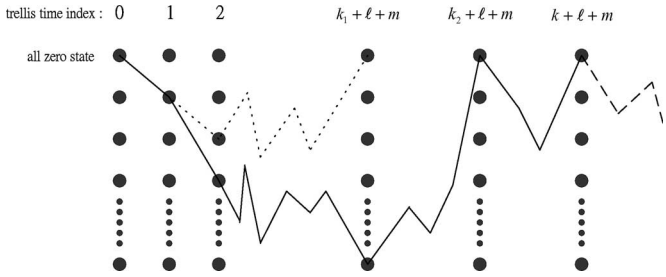

Fig. 2. Error-free path (solid line) of a convolutional codeword over its trellis diagram. Parameters k, ℓ, and m are the true message length, the number of CRC bits, and the memory order of the convolutional code, respectively.

is passed for some false length k_i is $2^{-\ell}$. Accordingly, it is reasonable to anticipate that by choosing ℓ large enough, the false length probability, as well as the block error probability, shall be made smaller than the system requirement. Unfortunately, such anticipation is only possibly true when the length offset $|k - k_i|$ is not less than ℓ, where k_i is a surmised wrong length and k is the true length.

In [4], it is shown by simulations that the false length probability is markedly larger than $2^{-\ell}$ when the length offset $|k - k_i|$ is smaller than ℓ, even if the convolutional coder perfectly recovers all channel errors. The NTT DoCoMo, thus, proposed to reverse the CRC bits before they are attached at the end of the message block, and showed by simulations that their proposal can reduce the false length probability to the desired $2^{-\ell}$ for length offsets smaller than ℓ under error-free transmission [4].

In [8], we proposed an alternative modification of the original CRC method by selectively flipping some of the CRC bits. We then derived a necessary and sufficient condition for the selection of flip polynomials, with which the false length probability can be reduced to zero (and hence, is already minimized) for every message length offset smaller than the number of CRC bits under the assumption that the transmission is error free.

In this paper, we further extend our result in [8] by additionally considering the effect of the inner convolutional coder. As a result, the necessary and sufficient condition for the selection of flip polynomials is generalized to include the impact of the convolutional coder. We also found that the length offset range of zero false length probability conditioning on the true message length is extended from $\ell - 1$ to $\ell + m - 1$. Moreover, an upper bound and a lower bound of the overall false length probability with respect to a uniform pick of the true message length from a candidate message length set $\mathcal{K} = \{k_1, k_2, \ldots, k_p\}$ are derived, and subsequently, confirmed numerically that the two bounds almost coincide for moderate $(\ell + m)$ value. Comparison of the block error performance between the proposed flip CRC method and the DoCoMo's reverse CRC method is also provided. Detail discussion will be given in Section IV.

The rest of the paper is organized as follows. The system model, the joint convolutional/CRC decoding strategy, and the flip CRC method proposed are addressed in Section II. The bounds for overall false length probability with respect to a uniform pick of the true message length is derived in Section III. Section IV summarizes and remarks the simulation results. Section V concludes the paper.

II. System Model and the Flip CRC Modification

Referring to Fig. 1, the candidate message length set $\mathcal{K} \triangleq \{k_1, k_2, \ldots, k_p\}$ is priorly negotiated between the transmitter and the receiver. Then, a true message block with k bits, where $k \in \mathcal{K}$, is CRC encoded by an ℓ-bit CRC encoder, followed by the encoding of an $(n, 1, m)$ convolutional encoder. Additional m zeros are padded after the CRC-encoded message block so as to terminate the trellis of the convolutional code. To alleviate the interference to other users, the transmission power is turned off after the transmission of the encoded data is completed. Finally, a Viterbi decoder and a CRC decoder jointly operate to decode the message bits without the knowledge of the true message block length k.

The idea behind the joint decoding of the convolutional decoder and the CRC decoder can be described as follows. Referring to the Viterbi decoding trellis in Fig. 2, since m zeros are padded at the end of the CRC-encoded message block of length $(k + \ell)$, the path that gives the smallest metric should end at the all-zero state at time index $(k + \ell + m)$ under error-free transmission. The CRC test, when applied to the convolutional decoded message up to level $(k + \ell + m)$, validates the integrity of the message block, and implicitly confirms its length. As a result, if the correct trellis path that corresponds to the transmitted convolutional codeword ends at the all-zero state at some time index $(k_2 + \ell + m)$ smaller than the correct time index $(k + \ell + m)$, the CRC test will be applied to invalidate the surmised message block length k_2. When an incorrect path ending at the all-zero state at level $(k_1 + \ell + m)$ has smaller path metric than the correct path due to the introduction of noise, the result of the CRC decoder will be used to prevent from a wrong estimate k_1 of the true message length k. Accordingly, a false length is claimed only when the convolutional decoder and the CRC decoder simultaneously fail to indicate such fault.

In [7] and [9], variations of the length detection strategy under the joint operation of the Viterbi decoder and the CRC

decoder have been proposed. Okumura and Adachi [7] proposed to perform a threshold test on a variable

$$\delta(k) \triangleq -10 \log \left(\frac{\lambda_0(k) - \lambda_{\min}(k)}{\lambda_{\max}(k) - \lambda_{\min}(k)} \right) \tag{1}$$

where $\lambda_{\max}(k)$ and $\lambda_{\min}(k)$ are, respectively, the maximal and the minimal path metric values among all survivors that end at trellis time index $(k + \ell + m)$ and $\lambda_0(k)$ is the path metric value for the survivor path ending at the all-zero state at level $(k + \ell + m)$. It needs to be pointed out that in Okumura and Adachi's system, the Viterbi decoder searches for the convolutional codeword that gives the largest path metric rather than the smallest.

Apparently, $\delta(k)$ equals zero in noiseless transmission if k is the true message length. However, $\delta(k)$ may be strictly greater than zero in a noisy environment, and the probability of detection may become unacceptably small due to a moderate noise if a strict condition as that k_i is a legitimate length for subsequent CRC test only when $\delta(k_i) = 0$ is adopted by the convolutional decoder. For this reason, Okumura and Adachi proposed to relax the strict condition to that $\delta(k_i) < \Delta$ for some positive Δ, where Δ is a system design parameter. Specifically, if $\delta(k_i) < \Delta$, the Viterbi decoder traces back the trellis to find the message block corresponds to the survivor path ending at the all-zero state at level $(k_i + \ell + m)$, and the CRC test is subsequently applied to the message block to check whether k_i is a candidate detected length. In the end, among all the candidate detected lengths, the one with the smallest δ function value will be chosen as the final estimate of the true message block length k.[1] Notably, since the input to the Viterbi decoder becomes pure noise after the correct trellis time index $(k + \ell + m)$, and since to output a surmised message length larger than k requires its δ function value strictly less than $\delta(k)$ with a valid CRC test result, it is statistically unlikely to yield a length estimate larger than k.

From the jointly decoding strategy described previously, the error events can be classified into two categories: *undetected error* and *detected error*. The former corresponds to the condition that an estimate of the true message block length is found, but a wrong message block is resulted. The latter concerns the situation that the joint decoder fails to find an estimate of the true message block length, and thus, receiver generates no output. The *undetected error events* can be further subdivided into that a wrong length is claimed, and that a wrong message block with correct length is resulted. We can, therefore, define four kinds of errors as

$$\begin{aligned} \text{DER} &\triangleq N_1/N \\ \text{FLR} &\triangleq N_2/N \\ \text{UER} &\triangleq (N_2 + N_3)/N \\ \text{BLER} &\triangleq (N_1 + N_2 + N_3)/N \\ &= \text{DER} + \text{UER} \end{aligned}$$

where N, N_1, N_2, and N_3 are the total number of message block samples experimented, the number of samples for which the receiver fails to output an estimate of the true message block length, the number of samples for which the receiver claims a wrong length, and the number of samples for which the receiver claims a wrong message block with the correct length, respectively, and DER and FLR are the detected error rate and false length rate, respectively. In addition, we denote by $\text{FLR}(i|k)$ as the conditional false length rate of message length offset i given that the true message length is k, where the message length offset is defined as the difference between the estimate message length and the true message length k.

In the following, a novel CRC modification by selectively flipping part of the CRC bits is introduced. Specifically, for a given ℓ-bit CRC, we construct a flip polynomial of degree $(\ell - 1)$, denoted by $f_\ell(x) = t_\ell x^{\ell-1} + \cdots + t_1$, where $t_j \in \{0, 1\}$ for $1 \le j \le \ell$. Then, the jth parity bits p_j is "flipped" (i.e., complemented) when $t_j = 1$, and "unflipped" (i.e., unchanged) otherwise. For clarity, the encoding and decoding rules of the flip CRC modification with respect to CRC generator polynomial $g_\ell(x)$ and its corresponding flip polynomial $f_\ell(x)$ are provided next.

1) *Encode a message block with k bits*
   a) For a message block $[m_k, \ldots, m_1]$, determine its corresponding ℓ parity check bits $[p_\ell, \ldots, p_1]$ such that $g_\ell(x) \,|\, \big(x^\ell M(x) + P(x)\big)$, where $M(x) = m_k x^{k-1} + \cdots + m_1$, $P(x) = p_\ell x^{\ell-1} + \cdots + p_1$, and "$a(x)|b(x)$" means that $a(x)$ divides $b(x)$.
   b) Flip the ℓ parity check bits according to the flip polynomial $f_\ell(x)$. The resultant parity check vector is $[\bar{p}_\ell, \ldots, \bar{p}_1] = [p_\ell \oplus t_\ell, \ldots, p_1 \oplus t_1]$, where "$\oplus$" represents modulo-2 addition.
   c) Attach the flipped ℓ parity check bits at the end of the k message bits to form a coded block of $[m_k, \ldots, m_1, \bar{p}_\ell, \ldots, \bar{p}_1]$ for subsequent convolutional encoding.
2) *Decode a candidate block with $(\hat{k} + \ell)$ bits that are passed from the convolutional decoder*
   a) Upon the reception of a message block $[r_{\hat{k}+\ell}, \ldots, r_1]$, calculate the ℓ parity check bits $[\hat{p}_\ell, \ldots, \hat{p}_1]$ for the surmised message block $[r_{\hat{k}+\ell}, \ldots, r_{\ell+1}]$.
   b) If $[\hat{p}_\ell \oplus t_\ell, \ldots, \hat{p}_1 \oplus t_1] = [r_\ell, \ldots, r_1]$, then the CRC test for message length $\hat{k}$ is passed; otherwise, it is not passed.

In [8], we provide a necessary and sufficient condition for the selection of flip polynomials that guarantee the conditional FLR to be zero for all message length offsets in $\{1, 2, \ldots, \ell - 1\}$ under error-free transmission and absence of convolutional coding protection. We further show that if the message block is uniformly distributed given the message length, the conditional FLR for our flip CRC modification is equal to $2^{-\ell}$ for all message length offsets not less than ℓ.

[1]The choice of the threshold value Δ will affect the BLER, the UER, and the number of tracebacks in the Viterbi decoder. It was shown by simulations [9] that as long as Δ is sufficiently large, its influence on the BLER and the UER is mild. Indeed, when $\Delta = \infty$, the receiver will examine the validity of the CRC test for all candidate message lengths in $\mathcal{K}$ and output the CRC-valid one with the smallest δ function value.

In this paper, we further enhance the result by considering the performance of the joint decoding of the convolutional decoder and the CRC decoder. As mentioned before, two tests—δ threshold test and CRC test—are simultaneously used to identify the message length. The next theorem then indicates that the inner convolutional code can not only significantly reduce the conditional FLR, but can also enlarge the zero-conditional-FLR margin from $\ell-1$ to $\ell+m-1$ under error-free transmission. Even though the following analysis is derived under the assumption of error-free transmission, simulations show that at moderate SNRs ($\geq$5.5 dB, as shown in Fig. 4), where channel transmission errors occur mildly during the convolutional decoding process, the conditional FLR remains almost intact as the next theorem tells.

Theorem 1: Assume error-free transmission and a consecutive candidate message length set $\mathcal{K}=\{k_1,k_2,k_3,\ldots\}=\{k_1,k_1+1,k_1+2,\ldots\}$, where $k_1\geq \ell+m$.[2] Also assume that the generator polynomial $g_\ell(x)$ satisfies $\gcd\left(g_\ell(x),x^i\right)=1$ for each $0\leq i\leq \ell+m-1$ and $\deg(g_\ell(x))=\ell$. Let the message block be uniformly distributed given the true message length k. Then, the joint decoding of the convolutional code and the flip CRC code gives the following[3]

1) $\mathrm{FLR}\left(i|k\right)=0$ for $1\leq i<\ell+m$ if and only if

$$\deg\left(\text{Remainder of}\left\{\frac{(1+x^i)f_\ell(x)}{g_\ell(x)}\right\}\right)\geq i-m \quad \text{for } 1\leq i<\ell+m. \tag{2}$$

2) $\mathrm{FLR}\left(i|k\right)=2^{-(\ell+m)}$ for $\ell+m\leq i<k$.

Proof: Since $\delta(k)=0$ in the absence of channel noise, the false length event can occur only possibly for $k_1\leq k_j<k$ with $\delta(k_j)=0$, regardless of the threshold value Δ.

Denote the input of the convolutional encoder by $[c_{k+\ell+m},\ldots,c_{m+1},c_m,\ldots,c_1]=[c_{k+\ell+m},\ldots,c_{m+1},0,\ldots,0]$, where the last m zeros are used to terminate the convolutional code. Let $C_0(x)\stackrel{\triangle}{=}\sum_{j=0}^{k+\ell-1}c_{m+1+j}x^j$; hence, $g_\ell(x)|(C_0(x)+f_\ell(x))$. Then

$$\begin{aligned}&\mathrm{FLR}(i|k)\\&=\Pr\left\{\mathbf{C}_i'\text{can pass the CRC test and }\delta(k-i)=0\right\}\\&=\Pr\left\{\mathbf{C}_i'\text{can pass the CRC test and }\mathbf{C}_i''=\mathbf{0}\right\}\\&=\Pr\left\{\mathbf{C}_i''=\mathbf{0}\right\}\Pr\left\{\,\mathbf{C}_i'\text{ can pass the CRC test}|\,\mathbf{C}_i''=\mathbf{0}\right\}\end{aligned}$$

where $\mathbf{0}\stackrel{\triangle}{=}[0,\ldots,0]$ is the all-zero vector, $\mathbf{C}_i'\stackrel{\triangle}{=}[c_{k+\ell+m},\ldots,c_{m+i+1}]$, $\mathbf{C}_i''\stackrel{\triangle}{=}[c_{m+i},\ldots,c_{i+1}]$, and $1\leq i<k$. By the three assumptions of: 1) uniformly distributed message, 2) $\gcd(g_\ell(x),x^i)=1$ for $0\leq i\leq \ell+m-1$, and 3) $\deg(g_\ell(x))=\ell$, we have[4] $\Pr\{\mathbf{C}_i''=\mathbf{0}\}=2^{-\min\{i,m\}}>0$. Hence, $\mathrm{FLR}(i|k)=0$ if and only if $\Pr\{\mathbf{C}_i'$ can pass the CRC test$|\mathbf{C}_i''=\mathbf{0}\}=0$.

Observe that for $1\leq i<\ell+m$, $\mathbf{C}_i'$ can pass the CRC test given that $\mathbf{C}_i''=\mathbf{0}$ if and only if

$$\begin{aligned}&g_\ell(x)|C_i'(x)+f_\ell(x)\\&\Leftrightarrow g_\ell(x)|x^i\left(C_i'(x)+f_\ell(x)\right)\\&\Leftrightarrow g_\ell(x)|C_0(x)+\left(c_{m+i}x^{i-1}+\cdots+c_{m+1}\right)+x^if_\ell(x)\\&\Leftrightarrow\begin{cases}g_\ell(x)|[(x^i+1)f_\ell(x)\\+(c_ix^{i-m-1}+\cdots+c_{m+1})], & \text{if } m+1\leq i<\ell+m\\ g_\ell(x)|(x^i+1)f_\ell(x), & \text{if } 1\leq i<m+1\end{cases}\end{aligned} \tag{3}$$

where the second step follows from $\gcd(g_\ell(x),x^i)=1$ for $0\leq i\leq \ell+m-1$, and the last step holds since $\mathbf{C}_i''=\mathbf{0}$ and $g_\ell(x)|(C_0(x)+f_\ell(x))$. Thus, $\mathrm{FLR}(i|k)=0$ for every $1\leq i<\ell+m$ if and only if (3) is violated for every $1\leq i<\ell+m$, which completes the proof of (2).

For $\ell+m\leq i<k$, $\mathbf{C}_i'$ and $\mathbf{C}_i''$ contain no parity check bits, and therefore, are independent of each other. Consequently,

$$\begin{aligned}&\mathrm{FLR}(i|k)\\&\quad=\Pr\left\{\mathbf{C}_i''=\mathbf{0}\right\}\Pr\left\{\mathbf{C}_i'\text{can pass the CRC test}\right\}\\&\quad=2^{-m}\cdot 2^{-\ell}=2^{-(\ell+m)}.\end{aligned}$$

In the previous theorem, the candidate message length set $\mathcal{K}$ is assumed to be consecutive so that the length offset i can be any positive number. It can be similarly proved that if $k_j\neq k_{j-1}+1$ for some j, where $\mathcal{K}=\{k_1,k_2,\ldots,k_p\}$ with $k_1<k_2<\cdots<k_p$, then the theorem statement should be modified as followings:

1) $\mathrm{FLR}(i|k_j)=0$ for all $i\notin\mathcal{K}_j\stackrel{\triangle}{=}\{i:i=k_j-k_u$ for some $1\leq u<j\}$ (since the receiver knows that the transmitter will not use any length outside $\mathcal{K}$).
2) $\mathrm{FLR}(i|k_j)=0$ for $1\leq i<\ell+m$ and $i\in\mathcal{K}_j$ if and only if

$$\deg\left(\text{Remainder of}\left\{\frac{(1+x^i)f_\ell(x)}{g_\ell(x)}\right\}\right)\geq i-m \quad \text{for } 1\leq i<\ell+m \text{ and } i\in\mathcal{K}_j.$$

3) $\mathrm{FLR}(i|k_j)=2^{-(\ell+m)}$ for $\ell+m\leq i<k_j$ and $i\in\mathcal{K}_j$.

For given m,ℓ, and $g_\ell(x)$, the legitimate flip polynomial $f_\ell(x)$ that satisfies (2) can be exhaustively searched by computers. For an 8-bit CRC protection with $g_8(x)=x^8+x^7+x^4+x^3+x+1$ and $(2,1,8)$ convolutional codes, i.e., $\ell=8$ and $m=8$, the number of flip polynomials satisfying (2) is 66. It is worth mentioning that the conditional FLR formula in Theorem 1

[2]It can be verified that when $k<\ell+m$, $\mathrm{FLR}(i|k)=0$ for $1\leq i<k$ if and only if $\deg$ (Remainder of $\{(1+x^i)f_\ell(x)/g_\ell(x)\}\}\geq i-m$ for $1\leq i<k$. Since no existing standards have specified their candidate message lengths smaller than the adopted $(\ell+m)$, we exclude this case from Theorem 1 (and its proof) to reduce the reading burden.

[3]The degree of a zero polynomial $h(x)=0$ is treated as $-\infty$; hence, $\deg$(Remainder of $\{(1+x^i)f_\ell(x)/g_\ell(x)\}\}\geq i-m$ at $1\leq i\leq m$ is equivalent to state that $(1+x^i)f_\ell(x)$ cannot be divided by $g_\ell(x)$ at $1\leq i\leq m$.

[4]Because parity bits $[c_{m+\ell},\ldots,c_{m+1}]$ are uniformly distributed under the three assumptions, $\Pr\left\{\mathbf{C}_i''=\mathbf{0}\right\}=2^{-\min\{i,m\}}$ for $1\leq i<\ell$ and $\ell+m\leq i<k$. It can also be shown under the same assumptions that for $\ell\leq i<\ell+m$, $[c_{\ell+m},\ldots,c_{i+1}]$ is uniformly distributed given that $[c_{m+i},\ldots,c_{\ell+m+1}]=\mathbf{0}$. Hence, for $\ell\leq i<\ell+m$, $\Pr\{\mathbf{C}_i''=\mathbf{0}\}=\Pr\{[c_{m+i},\ldots,c_{\ell+m+1}]=\mathbf{0}\}\times\Pr\{[c_{\ell+m},\ldots,c_{i+1}]=\mathbf{0}|[c_{m+i},\ldots,c_{\ell+m+1}]=\mathbf{0}\}=2^{-(i-\ell)}\cdot 2^{-\min\{\ell,m-i+\ell\}}=2^{-\min\{i,m\}}$.

cannot be improved, and hence, is optimal under uniformly distributed message and error-free transmission.

III. Performance Analysis for the FLR

In the previous section, we derived the formula for the conditional false length probability given the true message block length k, and proved that the flip CRC modification can minimize this probability for every i under error-free transmission. In this section, we will further examine the overall false length probability under uniformly distributed message length.

By assuming that the true message length is uniformly selected from $\mathcal{K} \stackrel{\triangle}{=} \{k_1, k_2, \ldots, k_p\}$,

$$\mathrm{FLR} = \frac{1}{p}\sum_{i=1}^{p} \Pr(E_i) \tag{4}$$

where E_i denotes the false length event given that the true message length is k_i.

Theorem 2: Assume error-free transmission and uniformly distributed message given the true message length. The overall false length rate under the assumption that the true message length is uniformly selected from $\mathcal{K} \stackrel{\triangle}{=} \{k_1, k_2, \ldots, k_p\}$, where $k_1 \geq \ell + m$, satisfies

$$\begin{aligned}&\mathrm{FLR}\\ &\geq \frac{1}{p}\sum_{i=1}^{p}\sum_{t=1}^{\left\lfloor \frac{k_i - k_1}{\ell+m}\right\rfloor} \left(2^{-t(\ell+m)} \times S(k_i - (\ell+m), t, \ell+m|\mathcal{K})\right.\\ &\quad \left.\times \left[1 - 2^{-(\ell+m)} \times [k_i - k_1 - (t+1)(\ell+m) + 1]^+\right]^+\right)\end{aligned} \tag{5}$$

and

$$\mathrm{FLR} \leq \frac{1}{p \cdot 2^{(\ell+m)}}\sum_{i=1}^{p} |\{k_j \in \mathcal{K} : k_j \leq k_i - \ell - m\}| \tag{6}$$

provided that a flip polynomial satisfying (2) is employed, where $S(u, t, d|\mathcal{K})$ is the number of choices of sets corresponding to the condition that "choose t distinct numbers from $\mathcal{K} \cap \{1, 2, \ldots, u\}$ such that any two must differ at least d," and $[a]^+ \stackrel{\triangle}{=} \max\{a, 0\}$.

Proof: Observe that under error-free transmission, the false length event for some k_j not equal to the true message length k_i occurs only when $\delta(k_j) \leq \delta(k_i) = 0$ if $k_1 \leq k_j < k_i$, and $\delta(k_j) < \delta(k_i) = 0$ if $k_i < k_j \leq k_p$. Since $\delta(k_j)$ is nonnegative, the aforementioned false length event can occur only when $\delta(k_j) = 0$ and $k_1 \leq k_j < k_i$. By Theorem 1, using a flip polynomial satisfying (2) implies that $\mathrm{FLR}(k_i - k_j|k_i) = 0$ for $k_i - \ell - m < k_j < k_i$, and $\mathrm{FLR}(k_i - k_j|k_i) = 2^{-(\ell+m)}$ for $k_1 \leq k_j \leq k_i - \ell - m$.

1) *Upper bound:* Let F_j denote the event that k_j is a legitimate candidate detected length that validates both the CRC test and $\delta(k_j) = 0$, provided that the true message length is k_i; thus, $\Pr(F_j) = \mathrm{FLR}(k_i - k_j|k_i)$. Then

$$\begin{aligned}&\Pr(E_i)\\ &= \Pr\left(\bigcup_{\{k_j \in \mathcal{K}:\, k_j \leq k_i - \ell - m\}} F_j\right)\\ &\leq \sum_{\{k_j \in \mathcal{K}:\, k_j \leq k_i - \ell - m\}} \Pr(F_j) \qquad (7)\\ &= |\{k_j \in \mathcal{K} : k_j \leq k_i - \ell - m\}| \cdot 2^{-(\ell+m)}. \qquad (8)\end{aligned}$$

Substituting (8) into (4) immediately gives (6).

2) *Lower bound:* Let $\mathcal{L}_{t,i}$ denote the event that there are t additional legitimate candidate detected lengths other than the true message length k_i. Then, the probability lower bound of $\Pr(\mathcal{L}_{t,i})$ can be derived as follows.

Let $\mathcal{A}_{t,i} \stackrel{\triangle}{=} \{k_{j_1}, k_{j_2}, \ldots, k_{j_t}\}$ be one of the possible appearances of t additional candidate detected lengths for the true message length k_i, and assume without loss of generality that $k_{j_1} < k_{j_2} < \cdots < k_{j_t} < k_i$. (Apparently, $\mathcal{L}_{t,i}$ is the union of all such possible $\mathcal{A}_{t,i}$.) Then, with probability 1, the lengths in $\mathcal{A}_{t,i}$ must differ by at least $(\ell + m)$, and are at most $(k_i - (\ell + m))$ according to Theorem 1. Put the $(\ell + m)$ expanding set of $\mathcal{A}_{t,i}$ as $\bar{\mathcal{A}}_{t,i} \stackrel{\triangle}{=} \{k \in \mathcal{K} : \bar{k} - (\ell+m) < k < \bar{k} + (\ell+m) \text{ for some } \bar{k} \in \mathcal{A}_{t,i}\}$, and let $\mathcal{B}_{t,i} = \{k \in \mathcal{K} : k \leq k_i - (\ell+m) \text{ and } k \notin \bar{\mathcal{A}}_{t,i}\}$. Thus,

$$\begin{aligned}&\Pr(\mathcal{A}_{t,i})\\ &= \Pr\left(\left(\bigcap_{k_j \in \mathcal{A}_{t,i}} F_j\right) \bigcap \left(\bigcap_{k_j \in \mathcal{B}_{t,i}} F_j^c\right)\right)\\ &= \left(\prod_{k_j \in \mathcal{A}_{t,i}} \Pr(F_j)\right) \times \Pr\left(\bigcap_{1 \leq j < j_1, k_j \in \mathcal{B}_{t,i}} F_j^c\right)\\ &\quad \times \Pr\left(\bigcap_{j_1 < j < j_2, k_j \in \mathcal{B}_{t,i}} F_j^c\right) \times \cdots\\ &\quad \times \Pr\left(\bigcap_{j_t < j < i, k_j \in \mathcal{B}_{t,i}} F_j^c\right)\\ &\geq 2^{-t(\ell+m)} \left[1 - \sum_{1 \leq j < j_1, k_j \in \mathcal{B}_{t,i}} \Pr(F_j)\right]^+ \times \cdots\\ &\quad \times \left[1 - \sum_{j_t < j < i, k_j \in \mathcal{B}_{t,i}} \Pr(F_j)\right]^+\\ &\geq 2^{-t(\ell+m)}\\ &\quad \times [1 - [k_{j_1} - k_1 - \ell - m + 1]^+ \cdot 2^{-(\ell+m)}]^+\\ &\quad \times [1 - [k_{j_2} - k_{j_1} - 2\ell - 2m + 1]^+ \cdot 2^{-(\ell+m)}]^+\\ &\quad \times \cdots\end{aligned}$$

$$\times [1-[k_i-k_{j_t}-2\ell-2m+1]^+\cdot 2^{-(\ell+m)}]^+$$
$$\geq 2^{-t(\ell+m)}\cdot$$
$$[1-[k_i-k_1-(t+1)(\ell+m)+1]^+\cdot 2^{-(\ell+m)}]^+ \quad (9)$$

where the first equality holds since $\Pr(F_j^c)=1$ for $k_j \notin \mathcal{A}_{t,i}\cup\mathcal{B}_{t,i}$ and $k_j \leq k_i-\ell-m$, the second equality follows the independence between F_u and F_v for $|k_u-k_v|\geq \ell+m$, (9) holds by oversumming all the integers outside $\bar{\mathcal{A}}_{t,i}$, and the last inequality holds since $[1-[a_1-c]^+\cdot b]^+\times[1-[a_2-c]^+\cdot b]^+\times\cdots\times[1-[a_{t+1}-c]^+\cdot b]^+\geq[1-[a_1+\cdots+a_{t+1}-c]^+\cdot b]^+$ for nonnegative $a_1,a_2,\ldots,a_{t+1},b$, and c.[5] As the earlier lower bound depends only on t and k_i,

$$\Pr(\mathcal{L}_{t,i})$$
$$\geq S(k_i-\ell-m,t,\ell+m|\mathcal{K})\times 2^{-t(\ell+m)}$$
$$\times\left[1-[k_i-k_1-(t+1)(\ell+m)+1]^+\cdot 2^{-(\ell+m)}\right]^+.$$

Consequently,

$$\Pr(E_i)$$
$$=\sum_{t=1}^{\infty}\Pr(\mathcal{L}_{t,i})$$
$$\geq \sum_{t=1}^{\left\lfloor\frac{k_i-k_1}{\ell+m}\right\rfloor} S(k_i-\ell-m,t,\ell+m|\mathcal{K})\times 2^{-t(\ell+m)}$$
$$\times\left[1-[k_i-k_1-(t+1)(\ell+m)+1]^+\cdot 2^{-(\ell+m)}\right]^+$$

and

$$\mathrm{FLR}$$
$$=\frac{1}{p}\sum_{i=1}^{p}\Pr(E_i)$$
$$\geq \frac{1}{p}\sum_{i=1}^{p}\sum_{t=1}^{\left\lfloor\frac{k_i-k_1}{\ell+m}\right\rfloor} S(k_i-\ell-m,t,\ell+m|\mathcal{K})$$
$$\times 2^{-t(\ell+m)}$$
$$\times\left[1-[k_i-k_1-(t+1)(\ell+m)+1]^+\cdot 2^{-(\ell+m)}\right]^+.$$

Both the derivations of the upper and the lower bounds rely on the union-bound argument, i.e., (7) and

$$\Pr\left(\bigcap_{j_1<j<j_2,k_j\in\mathcal{B}_{t,i}} F_j^c\right)\geq\left[1-\sum_{j_1\leq j<j_2,k_j\in\mathcal{B}_{t,i}}\Pr(F_j)\right]^+$$

which, from subsequent (8) and (9), can be expected to become loose when $(\ell+m)$ is too small. By depicting the upper and the lower bounds for $\mathcal{K}=\{39, 42, 49, 55, 58, 61, 65, 75, 81\}$ and $\mathcal{K}=\{101,102,\ldots,300\}$ in Fig. 3, where the former nonconsecutive candidate message length set is specified in the UMTS WCDMA specification [14, Table B.1 of Annex B], we found that the lower bound deviates from the upper bound only at small $(\ell+m)$, as expected, and this deviation becomes invisible when $(\ell+m)$ is beyond 10. In addition, the FLR decays exponentially as $(\ell+m)$ increases. It is worth mentioning that for a consecutive candidate message length set $\mathcal{K}=\{s,\ldots,s+p-1\}$, the two bounds reduce to only functions of p, and are no longer relevant to s.

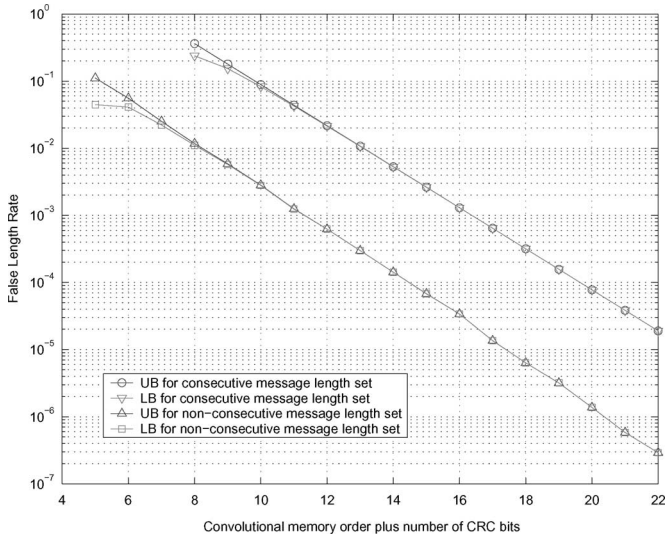

Fig. 3. The upper and the lower bounds of the FLR for different $(\ell+m)$ values for nonconsecutive message length set {39, 42, 49, 55, 58, 61, 65, 75, 81} and consecutive message length set {101,102,. . .,300}.

All the previous analyses are done under the error-free assumption, which results in $\mathrm{FLR}=\mathrm{UER}=\mathrm{BLER}$; however, these error rates are expectedly different in noisy communication. Their difference due to noise will be examined by simulations in the next section.

IV. Simulation Results

In this section, simulation results for antipodal transmission over the additive white Gaussian noise (AWGN) channel are presented. The (2,1,8) convolutional code with generator polynomial [561,753] (in octal) is employed in all simulations in Section IV-A and IV-B.

A. Simulations on Conditional FLR

In Fig. 4, the conditional FLRs for the DoCoMo's reverse CRC modification and the flip CRC modification are simulated at $\mathrm{SNR}=5.5$ dB. The convolutional memory order, the CRC bit number, and the true message length are, respectively, $m=8$, $\ell=8$, and $k=60$, and the length offset i can be any positive integer. Two flip polynomials are considered: $f_8(x)=x^7+x^5+x^3+x^2+1$ that satisfies (2), and $f_8(x)=x^7+1$ that violates (2) at $i=$12, 13, 14, 15.

[5]Specifically, we denote $a_1\triangleq k_{j_1}-k_1$, $a_2\triangleq k_{j_2}-k_{j_1}-(\ell+m)$, …, $a_t\triangleq k_{j_t}-k_{j_{t-1}}-(\ell+m)$, $a_{t+1}\triangleq k_i-k_{j_t}-(\ell+m)$, $b\triangleq 2^{-(\ell+m)}$, and $c\triangleq\ell+m-1$. Notably, $a_1\geq 0$, $a_2\geq 0$, …, $a_t\geq 0$, $a_{t+1}\geq 0$, with probability 1.

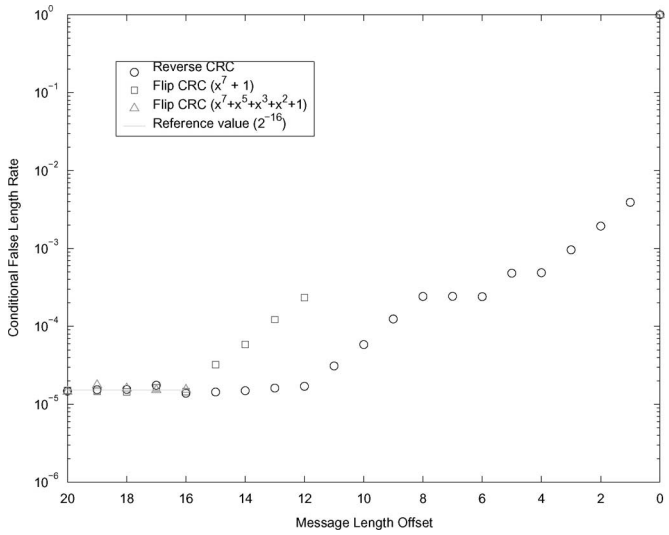

Fig. 4. Simulated conditional FLR at uncoded $\mathrm{SNR} = 5.5$ dB. The CRC code with $g_8(x) = x^8 + x^7 + x^4 + x^3 + x + 1$ are used. Two flip polynomials are tested: $f_8(x) = x^7 + x^5 + x^3 + x^2 + 1$ that satisfies (2) and $f_8(x) = x^7 + 1$ that violates (2) at message length offsets 12, 13, 14, 15. No points are drawn for the flip CRC methods at small length offsets, such as $1 \cdots 15$ for $f_8(x) = x^7 + x^5 + x^3 + x^2 + 1$ and $1 \cdots 11$ for $f_8(x) = x^7 + 1$, because the numbers of their fault length errors are much less than 100 in 10^8 simulation runs.

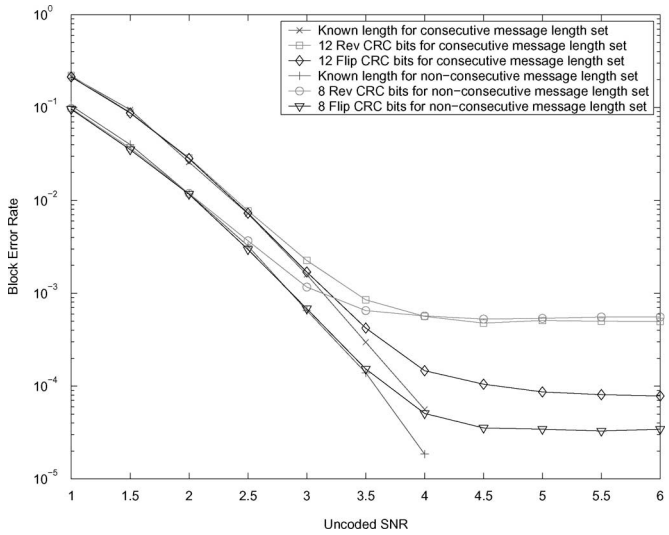

Fig. 5. Simulated BLERs for nonconsecutive message length set $\{39, 42, 49, 55, 58, 61, 65, 75, 81\}$ with CRC generator polynomial $g_8(x) = x^8 + x^7 + x^4 + x^3 + x + 1$ and flip polynomial $f_8(x) = x^7 + x^5 + x^3 + x^2 + 1$, and consecutive message length set $\{33, 34, \ldots, 232\}$ with CRC generator polynomial $g_{12}(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$ and flip polynomial $f_{12}(x) = x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x$. The curve labeled "known length" is the BLER given that the receiver knows the true message length.

We first noted that at uncoded $\mathrm{SNR} = 5.5$ dB, the performance of the flip CRC method with $f_8(x) = x^7 + x^5 + x^3 + x^2 + 1$ is almost identical to the error-free performance in Theorem 1. The figure also demonstrated the necessity of the condition in Theorem 1. The flip polynomial $f_8(x) = x^7 + 1$ that violates condition (2) at $i = 12$, 13, 14, and 15 gives apparently higher conditional FLR when the length offsets equal 12, 13, 14, and 15.

We have proved in [8] that in the absence of the inner convolutional coder, the DoCoMo's reverse CRC method flattens the conditional FLR to a constant value $2^{-\ell}$ for all message length offset under error-free transmission. However, Fig. 4 indicates that when the convolutional coder, as well as the AWGN noise, is additionally introduced into the system, their conditional FLR grows as the length offset decreases, and is markedly greater than $2^{-(\ell+m)}$ at small length offset. The conditional FLR of the proposed flip CRC method, on the contrary, remains unplotably small (i.e., smaller than the plot margin 10^{-6} of Fig. 4) at uncoded $\mathrm{SNR} = 5.5$ dB when the length offset is less than $(\ell + m)$.

B. Simulations on BLER, DER, UER, and FLR

In Figs. 5–8, we summarize the simulated BLER, DER, UER, and FLR performances for the DoCoMo's reverse CRC method and the proposed flip CRC method for a nonconsecutive candidate message length set $\{39, 42, 49, 55, 58, 61, 65, 75, 81\}$ and a consecutive candidate message length set $\{33,34,\ldots,232\}$. The system simulated is set as in Fig. 1.

We first examined the BLER degradation due to lack of message length information. In Fig. 5, the curve labeled "known length" represents the simulated BLER given that the receiver knows the true message length. We noted that when the SNR is low ($\leq$2.5 dB), both the flip CRC method and the DoCoMo's reverse CRC method perform close to that of known length system. Since the block error events at low SNRs occur mainly due to the failure of the convolutional decoder in correcting the channel errors, and are irrelevant to whether the true message length is known or not, it is reasonable that the BLER degradation due to lack of true message length information is small at low SNRs. When the SNR increases beyond 2.5 dB, the difference between known length BLER and unknown length BLERs, including those of the DoCoMo's reverse CRC method and the flip CRC method, becomes more evident, as anticipated. The BLERs of both the DoCoMo's reverse CRC method and the flip CRC method approach a floor value as the SNR further increases. However, the BLER error floor value of the flip CRC method is significantly smaller than that of the DoCoMo's reverse CRC method. Fig. 5 also hints that the BLER error floor value of the flip CRC method can be adjusted by adopting different CRC bit numbers and candidate message length sets.

We depict the simulation results for the DER in Fig. 6. It shows that the DER decreases exponentially fast as the SNR increases, and is almost indifferent with respect to the CRC modification methods. Another observation is that the DER dominates the BLER at low SNR, and becomes negligible for the calculation of the BLER when SNR grows beyond 5 dB (cf., Fig. 9).

The earlier observation can be further confirmed by the UER curves in Fig. 7. The comparison between the curves in Fig. 6 and 7 shows that the UER is much smaller than the DER at low SNR. However, the UER decreases at a much lower speed than the DER as the SNR increases, and approaches a floor value when the SNR is further increased. Therefore, it is the UER

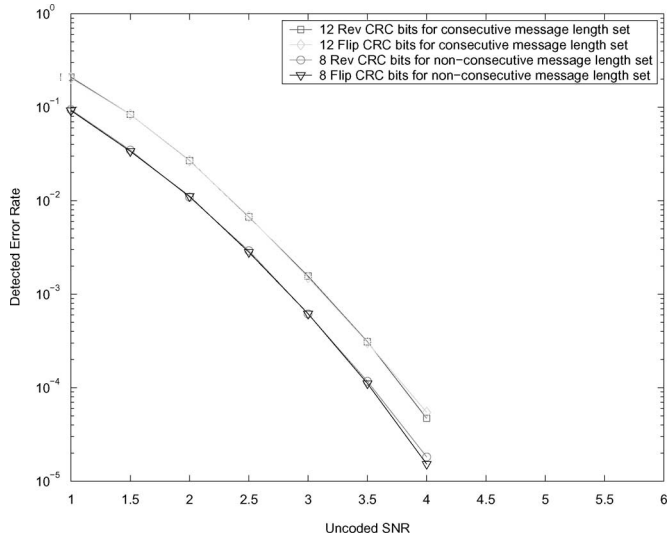

Fig. 6. Simulated results for the DER with the same setting as in Fig. 5.

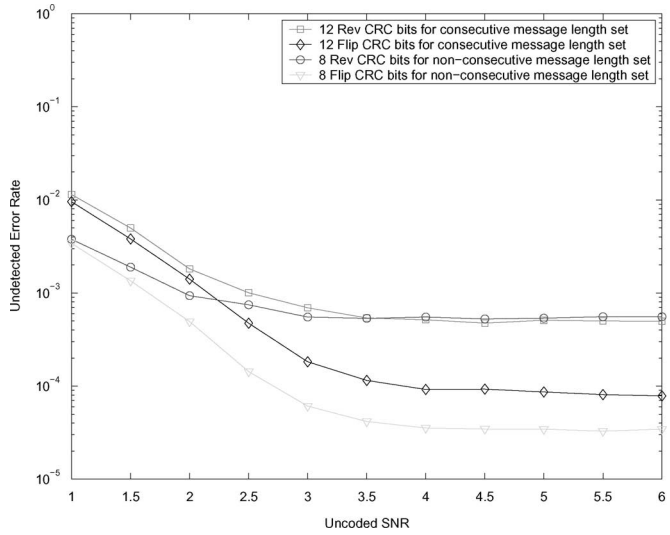

Fig. 7. Simulation results for the UER with the same setting as in Fig. 5.

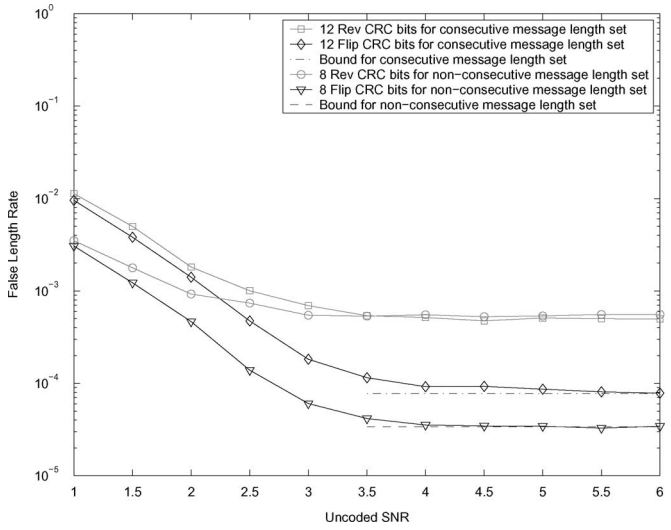

Fig. 8. Simulation results for the FLR with the same setting as in Fig. 5.

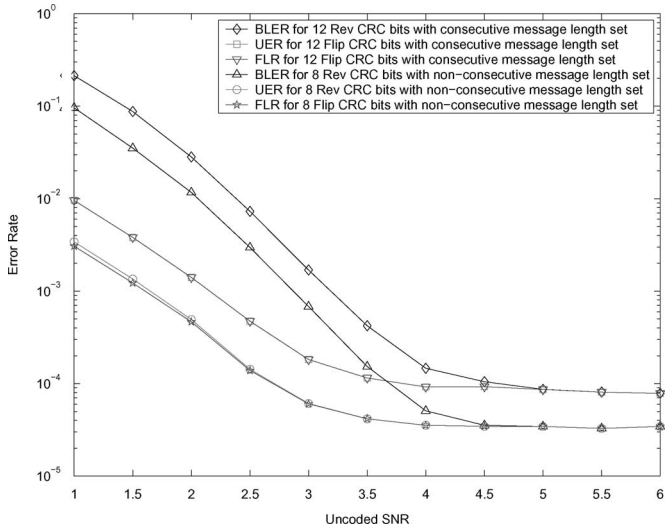

Fig. 9. Simulation results for the BLER, the UER, and the FLR with the same setting as in Fig. 5.

rather than the DER to decide the ultimate floor value of the BLER.

In Fig. 8, we obtained similar behavior for the FLR to that of the UER. Indeed, the FLR and the UER are close to each other for all simulated SNRs (cf., Fig. 9). The theoretical upper and the lower bounds[6] for the FLR, derived based on the assumption of error-free transmission, i.e., $\mathrm{SNR} = \infty$, are also plotted for comparison. As shown in the figure, the FLR floor value quickly approaches the bounds at moderate SNR, such as 5 dB, and will ultimately lie within the two bounds.

Finally, we summarized the previous simulated BLER, UER, and FLR in Fig. 9. As mentioned before, the UER and the FLR almost coincide for all SNRs simulated, but deviate from the BLER at low SNRs. In principle, the deviation of the BLER to the UER, which is exactly the DER, can be eliminated by system retransmission—a conventional system application of the CRC technique; hence, it is practical to expect that the ideal BLER curve for a system enhanced with retransmission scheme shall follow the UER/FLER curve. Finally, the UER, the FLR, and the BLER converge to the same floor value that can be *a priori* determined by the theoretical bounds in Theorem 2.

C. Simulations for Different Convolutional/CRC Combinations

We have shown in the previous section that the error floor of the BLER can be determined by the FLR bounds in Theorem 2, which, according to Fig. 3, is in turn adjustable by the $(\ell + m)$ value. Fig. 10 further examined the impact of different convolutional/CRC code combinations on the BLER when $(\ell + m)$ is fixed as 20. The candidate message length set simulated in this

[6]The two bounds are actually indistinguishable in Fig. 8. For consecutive message length set with $\ell + m = 20$, the upper bound and the lower bound are 7.7677×10^{-5} and 7.7672×10^{-5}, respectively. For nonconsecutive message length set with $\ell + m = 16$, the upper bound and the lower bound are 3.3908×10^{-5} and 3.3906×10^{-5}, respectively. Therefore, we simply plot the upper bound for comparison with the simulated results in Fig. 8.

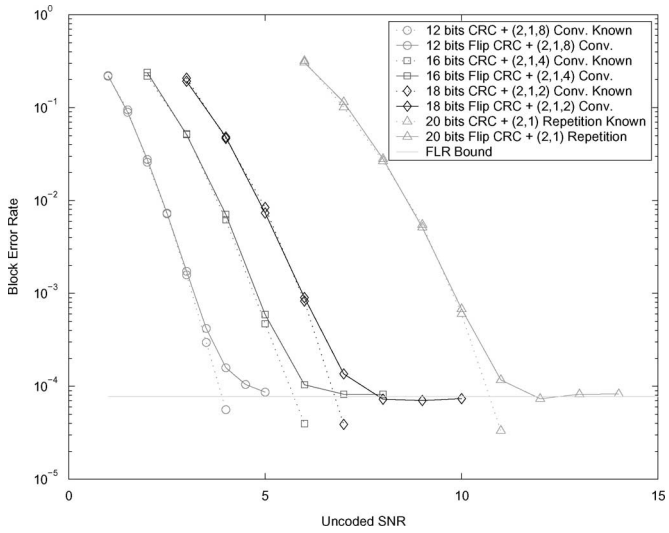

Fig. 10. Simulations for different convolutional/CRC combinations with fixed $\ell + m = 20$. The generator polynomials of the convolutional codes tested are [561 753], [46 72], and [75] (in octal) for $m = 8$, 4, and 2, respectively. The flip CRC codes tested include: 1) $g_{12}(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$ and $f_{12}(x) = x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x$, 2) $g_{16}(x) = x^{16} + x^{12} + x^5 + 1$ and $f_{16}(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$, 3) $g_{18} = x^{18} + x^{17} + x^{15} + x^{14} + x + 1$ and $f_{18}(x) = x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + 1$, 4) $g_{20}(x) = x^{20} + x^{19} + x^6 + x^5 + x^3 + 1$ and $f_{20}(x) = x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2$. The candidate message length set is $\mathcal{K} = \{33, 34, \ldots, 232\}$.

section is $\{33, 34, \ldots, 232\}$. Four different convolutional/CRC code combinations are tested.

Several observations can be made from Fig. 10. First, it is double confirmed that the BLER error floor is decided only by the $(\ell + m)$ value, and is independent of the convolutional/CRC code combinations. Second, all convolutional/CRC code combinations perform close to their respective known length system before they reach their BLER error floors. Notably, the BLER performance of the known length system is actually given by the performance of the convolutional codes. Third, the convolutional/CRC code combination with larger m value can yield better BLER performance. However, as the decoding complexity (such as the Viterbi algorithm) for convolutional codes increases exponentially with m, while the decoding complexity for CRC codes grows only linearly with ℓ, there is a tradeoff between the BLER performance (that prefers larger m) and the overall decoding complexity (that favors larger ℓ).

In a usual blind-length communication system, the BLER that equals the sum of the UER and the DER is often required to be less than a certain value at some target operating SNR. It is also common to specify a minimum UER requirement in order to differentiate the detected error events and the undetected error events for applications like automatic retransmission request (ARQ). A specific example is that the blind transport format detection of 3GPP WCDMA system particularizes the minimum BLER and the minimum UER as 10^{-2} and 10^{-4}, respectively [13, p. 39]. It should be noted that the UER defined in this paper is termed the *false detection rate* (FDR) in the 3GPP WCDMA standard.

Since the BLER performance curve can, in fact, be approximately given by the performance of the respective known length system and the FLR bounds (i.e., the BLER error floor), one may decide the system parameters in the following fashion.

Give the candidate message length set, the operating SNR, the minimum BLER, and the minimum UER required.

1) Search through all known length performance curves, and find the one that gives the smallest memory order m such that the BLER at the operating SNR (with appropriate SNR margin) is lower than the minimum BLER required.[7]
2) After determining m, decide the minimum number of CRC bits, i.e., ℓ, such that the FLR upper bound is smaller than the minimum UER required.

Through the aforementioned procedure, one can determine a pair of appropriate m and ℓ values that satisfy both the BLER and the UER requirements with the lowest decoding complexity for the joint convolutional/CRC decoder.

V. Conclusion

In this paper, we revisit our previously proposed flip CRC modification by considering the impact of joint decoding of the CRC code and the convolutional code. We found that the inner convolutional coder can not only largely extend the offset range of the zero conditional FLR, but can also exponentially reduce the conditional FLR value at those offsets at which the conditional FLR is not zero. A simple upper bound for the overall FLR is also provided, and is numerically shown to be almost tight for moderate $(\ell + m)$ value by means of a lower bound. Although the design criterion and the subsequent performance analyses of the flip CRC modification are established under the error-free assumption, their behaviors over a noisy environment have been examined by simulations in Figs. 4–10. Our simulations certify the feasibility of using CRC bits simultaneously for length detection and error detection in some specific applications like the UMTS WCDMA. The final observation, for which the BLER can be well approximated by the performance curve of the convolutional code below a certain SNR value, and approach a floor value determined well by the FLR bound beyond this SNR value, shall be useful in simplifying the design of the UMTS WCDMA system.

References

[1] F. Adachi, M. Sawahashi, and H. Suda, "Wideband DS-CDMA for next-generation mobile communications systems," *IEEE Commun. Mag.*, vol. 36, no. 9, pp. 56–69, Sep. 1998.
[2] D. Bertsekas and R. Gallager, *Data Networks*. Englewood Cliffs, NJ: Prentice-Hall, 1995.
[3] S. Lin and D. J. Costello, Jr., *Error Control Coding 2nd ed.* Upper Saddle River, NJ: Pearson/Prentice-Hall, 2004.
[4] NTT DoCoMo, *TSGR1#5(99)689* TSG-RAN Working Group1 Meeting #5, Cheju, Korea. Jun. 1999.

[7] Notably, the BLER performance curve for the known length system (equivalently, the performance curve for the convolutional code adopted) can be obtained either from the tables in [3] and [11] or by explicit simulations.

[5] Y. Okumura and F. Adachi, "Variable rate data transmission with blind rate detection for coherent DS-CDMA mobile radio," *Electron. Lett.*, vol. 32, no. 20, pp. 1865–1866, Sep. 1996.
[6] Y. Okumura and F. Adachi, "Variable rate transmission and blind rate detection for coherent DS-CDMA mobile radio," *Electron. Lett.*, vol. 33, no. 24, pp. 2026–2027, Nov. 1997.
[7] Y. Okumura and F. Adachi, "Variable-rate data transmission with blind rate detection for coherent DS-CDMA mobile radio," *IEICE Trans. Commun.*, vol. E81-B, no. 7, pp. 1365–1373, Jul. 1998.
[8] S.-L. Shieh, P.-N. Chen, and Y. S. Han, "A novel modification of cyclic redundancy check for message length detection," in *Proc. 2004 Int. Symp. Inf. Theory Appl.*, Parma, Italy, Oct. 10–13, pp. 178–183.
[9] S.-L. Shieh, S.-T. Kuo, P.-N. Chen, and Y. S. Han, "Strategies for blind transport format detection using cyclic redundancy check in UMTS WCDMA," in *Proc. 2005 IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Montreal, QC, Canada, Aug. 22–24, vol. 2, pp. 44–50.
[10] I. Sohn and S. Lee, "Blind rate detection algorithm in W-CDMA mobile receiver," in *Proc. 2001 IEEE Veh. Technol. Conf.*, Oct., pp. 1589–1592.
[11] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Englewood Cliffs, NJ: Prentice-Hall, 1995.
[12] 3rd Generation Partnership Project, "Multiplexing and channel coding (FDD)," 3GPP Tech. Spec. TS 25.212 V3.9.0, Mar. 2002.
[13] 3rd Generation Partnership Project, "Technical specification group radio access network; user equipment (UE) radio transmission and reception (FDD)," 3GPP Tech. Spec. TS 25.101 V5.8.0, Sep. 2003.
[14] 3rd Generation Partnership Project, "Services provided by the physical layer," 3GPP Tech. Spec. TS 25.302 V3.16.0, Sep. 2003.

Shin-Lin Shieh was born in Kinmen, Taiwan, R.O.C., in 1977. He received the B.Sc. and M.Sc. degrees in electrical engineering from the National Tsing-Hua University, Hsinchu, Taiwan, in 1999 and 2001, respectively. He is currently working toward the Ph.D. degree in the Department of Communications Engineering, National Chiao-Tung University, Hsinchu.

He was in the military service for three months. In 2002, he joined the Wireless Communication Technology Department, Computer and Communication Laboratory (CCL), Industrial Technology Research Institute (ITRI), Taiwan, where he was engaged in several projects on developing baseband communication algorithms. In 2005, he joined the Wideband Code Division Multiple Access (WCDMA) Project, Sunplus Technology Company, Ltd. He is currently with the Sunplus mMobile, Inc., Hsinchu, a subsidiary spun-off from the Sunplus Technology Company, Ltd., and is involved in designing baseband algorithms of enhanced data rates for global system for mobile communications evolution (EDGE), WCDMA, high-speed downlink packet access (HSDPA), and other communication systems. His current research interests include error-control coding, information theory, and wireless communications.

Po-Ning Chen (S'93–M'95–SM'01) was born in Taipei, Taiwan, R.O.C., in 1963. He received the B.Sc. and M.Sc. degrees from the National Tsing-Hua University, Hsinchu, Taiwan, in 1985 and 1987, respectively, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, in 1994, all in electrical engineering.

From 1985 to 1987, he was with the Image Processing Laboratory, National Tsing-Hua University, where he was engaged in the recognition of Chinese characters. He was in the military service for two years. In 1989, he joined Star Tech., Inc., where he developed the first prototype of fingerprint-recognition systems. He has also been a Vice General Manager at Wan Ta Technology, Inc., where he conducted several projects on point-of-sale systems. In 1995, he became a Research Staff in the Advanced Technology Center (ATC), Computer and Communication Laboratory (CCL), Industrial Technology Research Institute (ITRI), Taiwan, where he led a project on Java-based network managements. In 1996, he joined the Department of Communications Engineering, National Chiao-Tung University, Hsinchu, as an Associate Professor, and became a full Professor in 2001. His current research interests include information and coding theory, large deviations theory, distributed detection, and sensor networks.

Prof. Chen is the recipient of the 2000 Young Scholar Paper Award from the Academia Sinica, Taiwan.

Yunghsiang S. Han (S'90–M'93) was born in Taipei, Taiwan, R.O.C., on April 24, 1962. He received the B.S. and M.S. degrees in electrical engineering from the National Tsing Hua University, Hsinchu, Taiwan, in 1984 and 1986, respectively, and the Ph.D. degree in computer and information science from the School of Computer and Information Science, Syracuse University, Syracuse, NY, in 1993.

From 1993 to 1997, he was an Associate Professor in the Department of Electronic Engineering, Hua Fan College of Humanities and Technology, Taipei Hsien, Taiwan. From 1997 to 2004, he was with the Department of Computer Science and Information Engineering, National Chi Nan University, Nantou, Taiwan, where he was promoted to Full Professor in 1998. From June to October 2001, he was a Visiting Scholar in the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, and from September 2002 to January 2004, he was the SUPRIA Visiting Research Scholar in the Department of Electrical Engineering and Computer Science and CASE Center, Syracuse University. He is currently with the Graduate Institute of Communication Engineering, National Taipei University, Taipei, Taiwan. His current research interests include wireless networks, security, and error-control coding.

Prof. Han is the recipient of the 1994 Syracuse University Doctoral Prize.