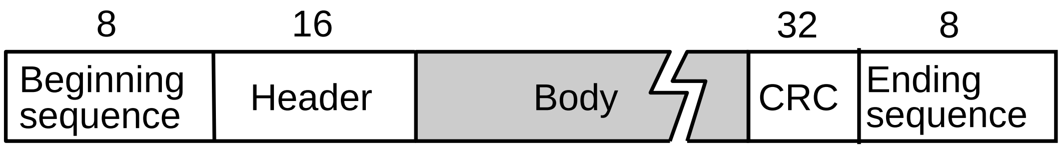
PERFORMANCE ESTIMATION OF CRC WITH LDPC CODES

Presenters: Rich Prodan and BZ Shen

PACKET ERROR DETECTION WITH CYCLIC REDUNDANCY CHECK (CRC)

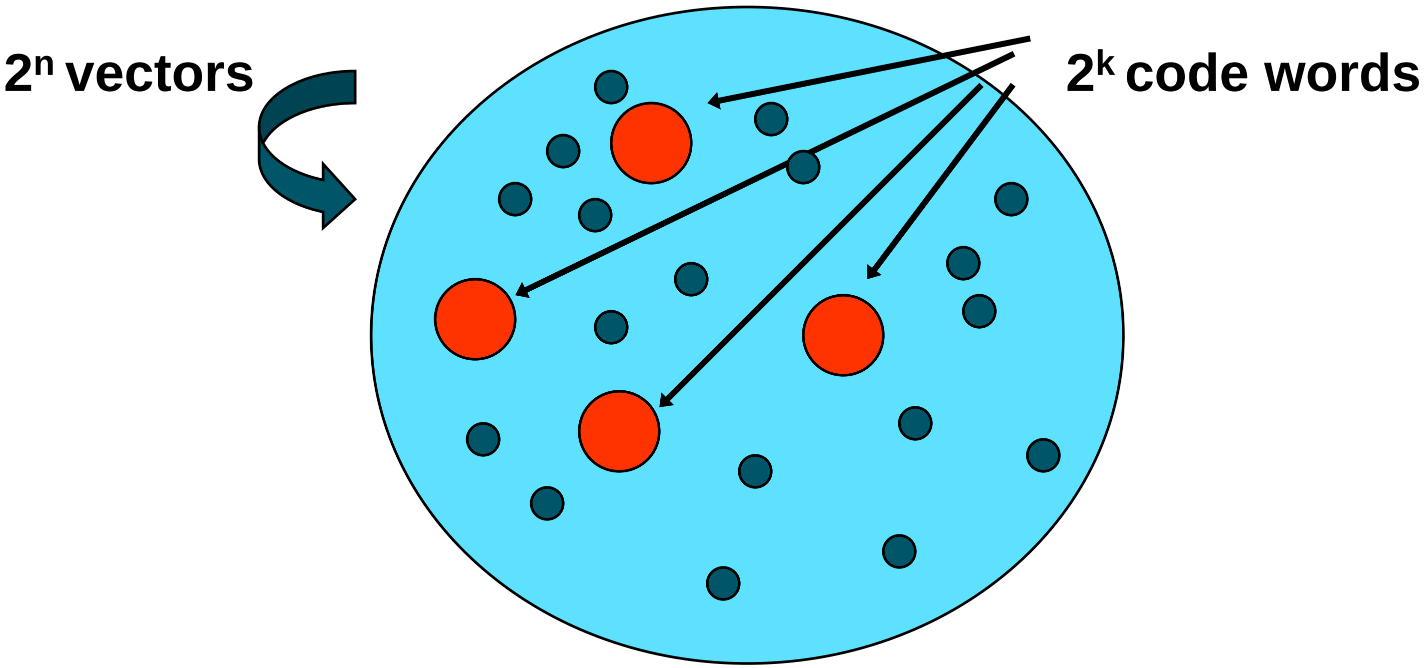
- **Add n-k bits of extra data (the CRC field) to an k-bit message to provide error detection function (i.e. an (n,k) binary cyclic code)**



- **For efficiency, n-k << n**
  - e.g., n-k = 32 for Ethernet and k = 12,000 (1500 bytes)

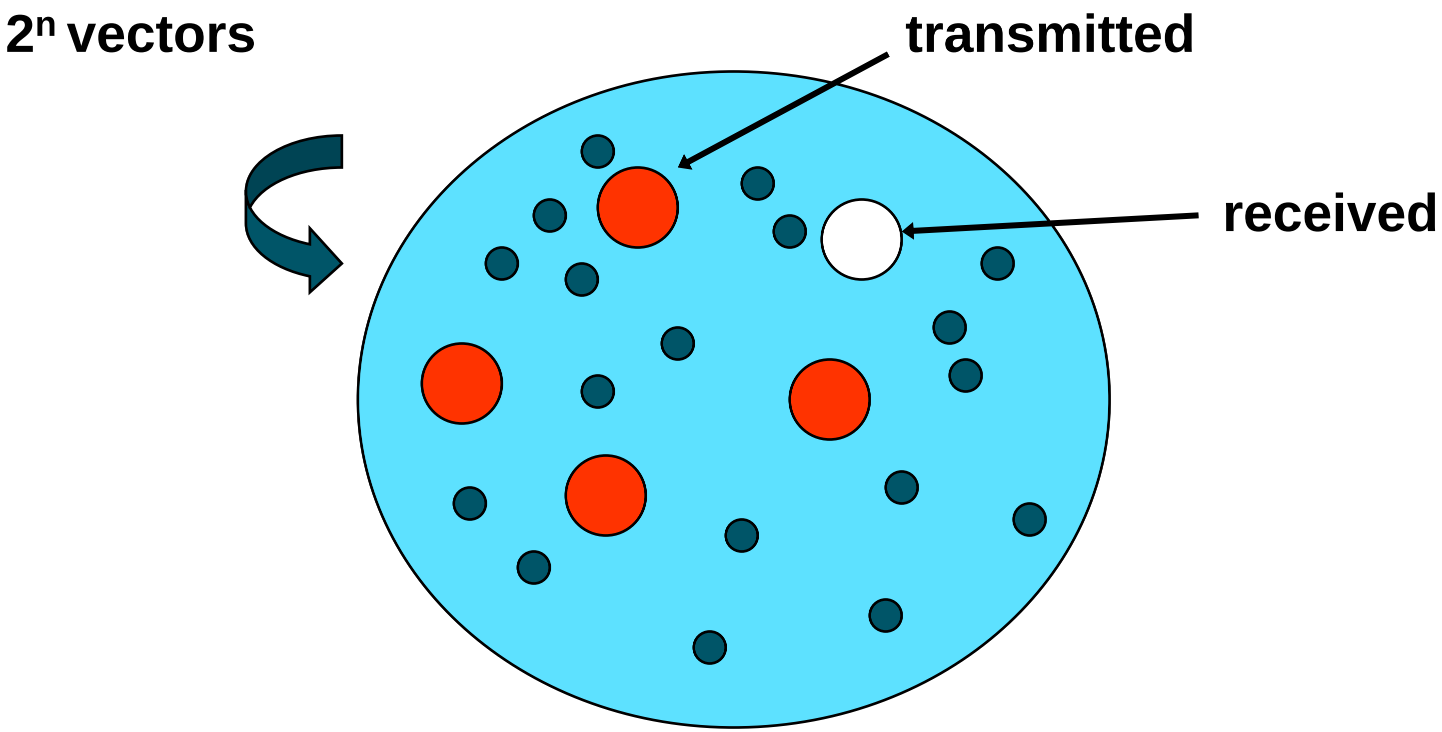
A PICTORIAL VIEW OF CRC CODING

Replace k information bits by a unique n bit code word



ERROR DETECTION

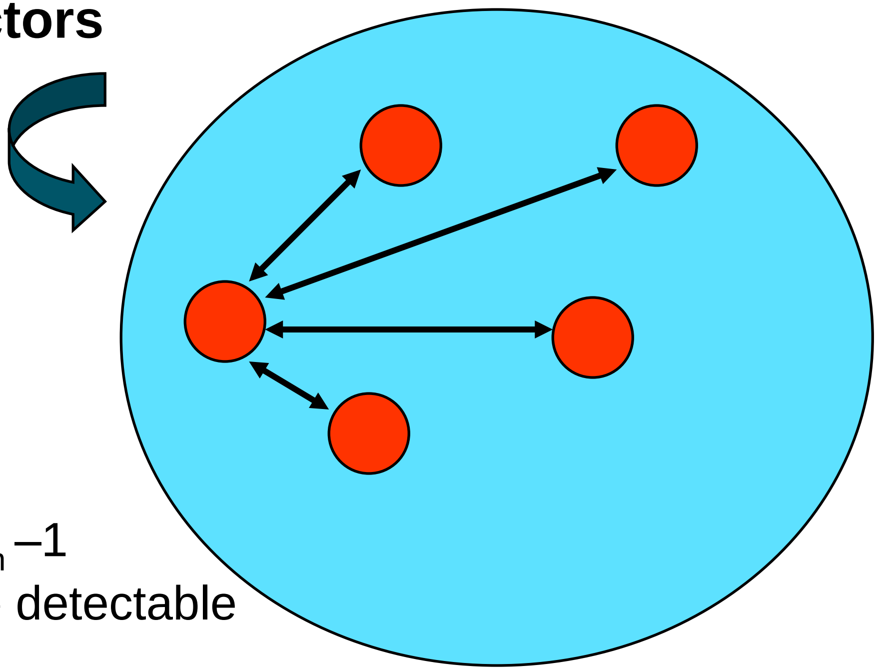
Received vector not equal to one of the 2^k code words



ERROR DETECTION CAPABILITY

code words differ in at least d_{min} positions

2^k vectors



up to $d_{min} - 1$
errors are detectable

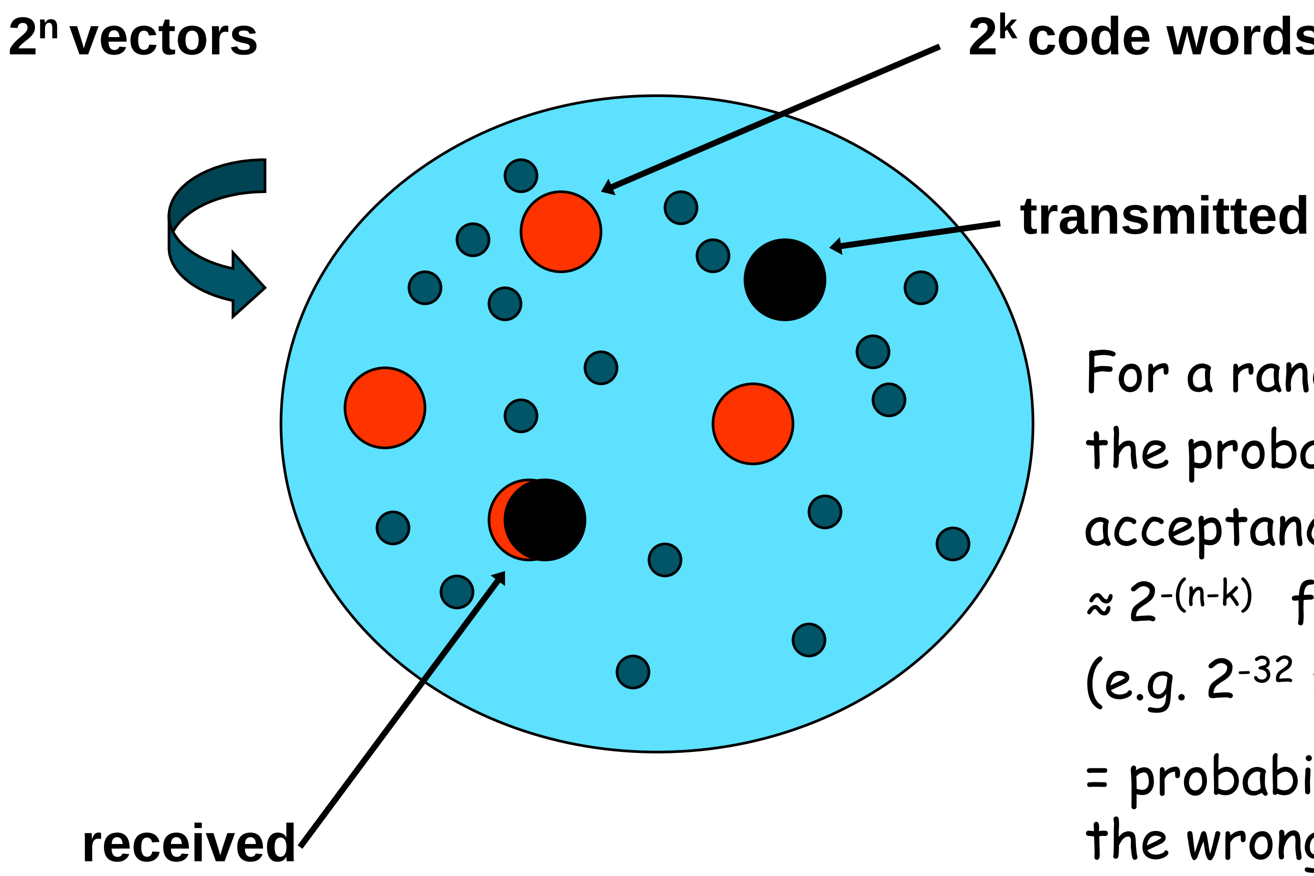
0xx1x0x0

4 differences

1xx0x1x1

$\leq$ 3 errors can be detected

MISDETECTION

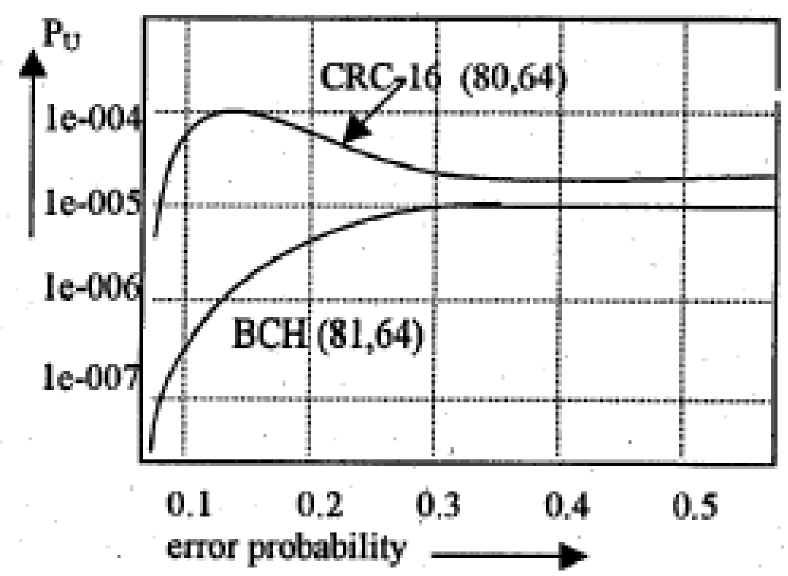


For a random vector:
the probability of false acceptance is $(2^k-1)/2^n$
$\approx 2^{-(n-k)}$ for $2^k \gg 1$
(e.g. 2^{-32} = 2.3e-10)

= probability of hitting the wrong code word (misdetection)

PROPER CODES

- **Linear block codes do not necessarily obey the $2^{-(n-k)}$ bound**
- **A code is proper if P_U is monotonically increasing in p for $0 \le p \le 0.5$**
- **Hamming codes and primitive double error-correcting BCH codes are proper**



$2^{-16} = 1.5e-5$

PROBABILITY OF UNDETECTABLE ERROR

- ***C*: binary [n, k] linear code**
  - n: the codeword length
  - k: the number of information bits
- ***p* : bit error probability on every received bit**
- **$P_{ue}(C, p)$: probability of undetectable error**

Among 2^n binary random strings of size n (i.e. $p=1/2$) there are 2^k strings are codewords of $C \rightarrow$ the fraction of such strings that are codewords of C is $2^k/2^n$. Thus

$$P_{ue}(C, \frac{1}{2}) = 2^{-(n-k)}$$

In general, it is not necessary true that $P_{ue}(C, p) \leq P_{ue}(C, \frac{1}{2})$ for $p < \frac{1}{2}$

EXISTENCE UPPER BOUND

Levenshtein bound (1977) For a given n and k, if $0 \leq p \leq 1/2$ and $R = k/n \leq 1 - H_2(p)$, then there is a binary [n, k] linear codes $\boldsymbol{C}$ such that

$$P_{ue}(C, p) \leq p^{n\rho(R)}(1-p)^{n-n\rho(R)}$$

where $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and $0 \leq \rho(\mathrm{R}) \leq 1/2$ such that $H_2(\rho(R)) = 1 - R$

The bound gives the best a CRC code can achieve. However, not all CRC codes have such upper bound.

GOOD CRC CODES

HD	IEEE 802.3 0x82608EDB {32}	Castagnoli (iSCSI) 0x8F6E37A0 {1,31}	Koopman 0xBA0DC66B {1,3,28}	Castagnoli 0xFA567D89 {1,1,15,15}	Koopman 0x992C1A4C {1,1,30}	Koopman 0x90022004 {1,1,30}	Castagnoli 0xD419CC15 {32}	Koopman 0x80108400 {32}
6	172-268	178-5243	**153-16360**	**275-32736**	**135-32737**	**8-32738**	82-1060	
5	269-2974	—	—	—	—	—	**1061-65505**	**8-65505**
4	**2975-91607**	**5244-131072...**	16361-114663	32737-65502	32738-65506	32739-65506	—	—

Philip Koopman, "32-Bit Cyclic Redundancy Codes for Internet Applications,"
The International Conference on Dependable Systems and Networks (DSN) 2002

ADDING CRC BITS TO LDPC INFORMATION BITS

- **On long size downstream/upstream (16200,14400) LDPC code**
  - After adding 32 bit CRC, the actual number of information bits is 14368
  - Need a (14400,14368) CRC code
- **On medium size upstream (5940, 5040) LDPC code**
  - After adding 32 bit CRC, the actual number of information bits is 5008
  - Need a (5040,5008) CRC code
- **On short size upstream (1120, 840) LDPC code**
  - After adding 32 bits CRC, the actual number of information bits is 808
  - Need a (840,808) CRC code

ON DOWNSTREAM LDPC CODE (4096 QAM)

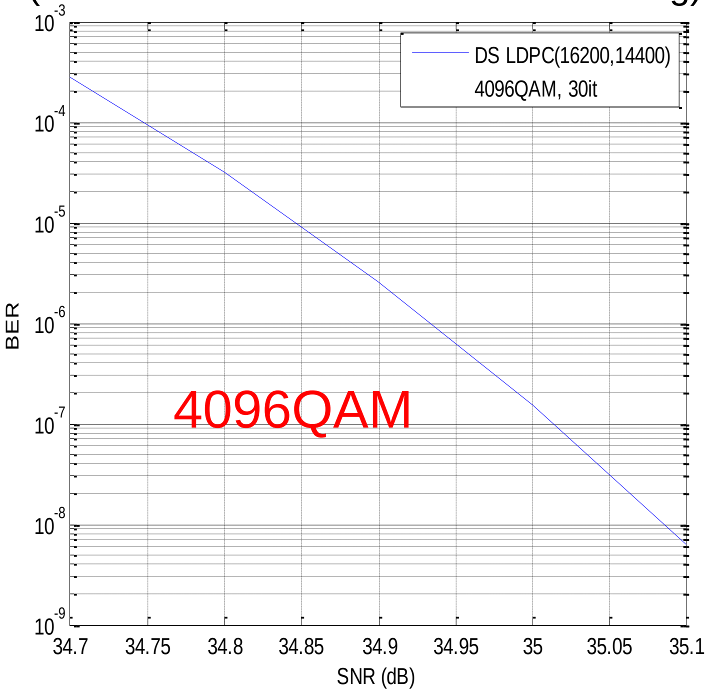
$$\text{LDPC code information} : 14368\ bits$$

$$32\ \text{bits CRC} : (n,k) = (14400,14368) \Rightarrow \text{CRC rate} : R = 0.99778$$

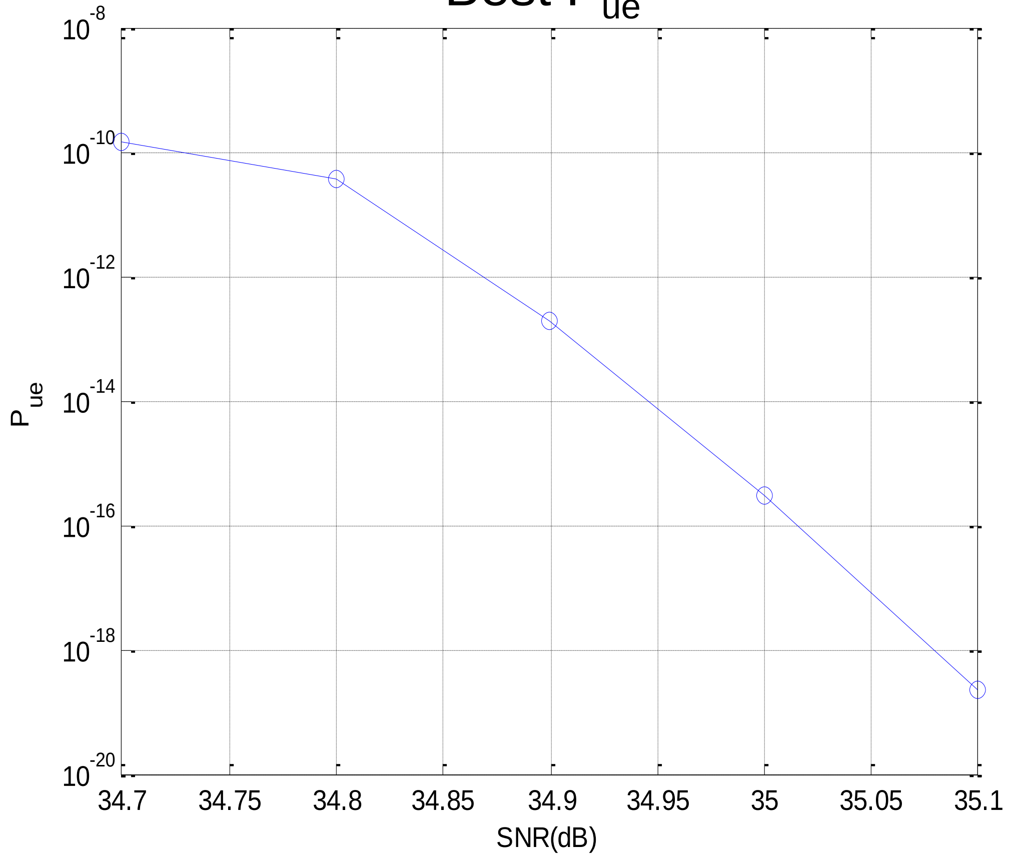
$$1 - R = 0.022222 \rightarrow \rho(R) = 0.00015792905 \Rightarrow R \le 1 - H_2(p)\ \text{when}\ p \le 0.0001579$$

BER (bit error rate)

(after max. 30 iterations LDPC decoding)



Best P_{ue}



ON LONG SIZE UPSTREAM LDPC CODE (4096 QAM)

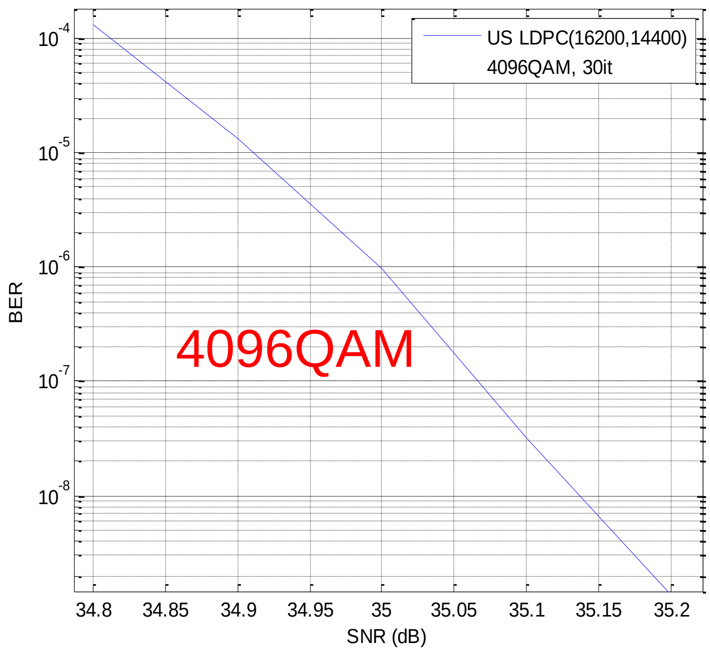
$$\text{LDPC code information}: 14400\ \textit{bits}$$

$$\text{32 bits CRC}: (n,k) = (14400,14368) \Rightarrow \text{CRC rate}: R = 0.99778$$

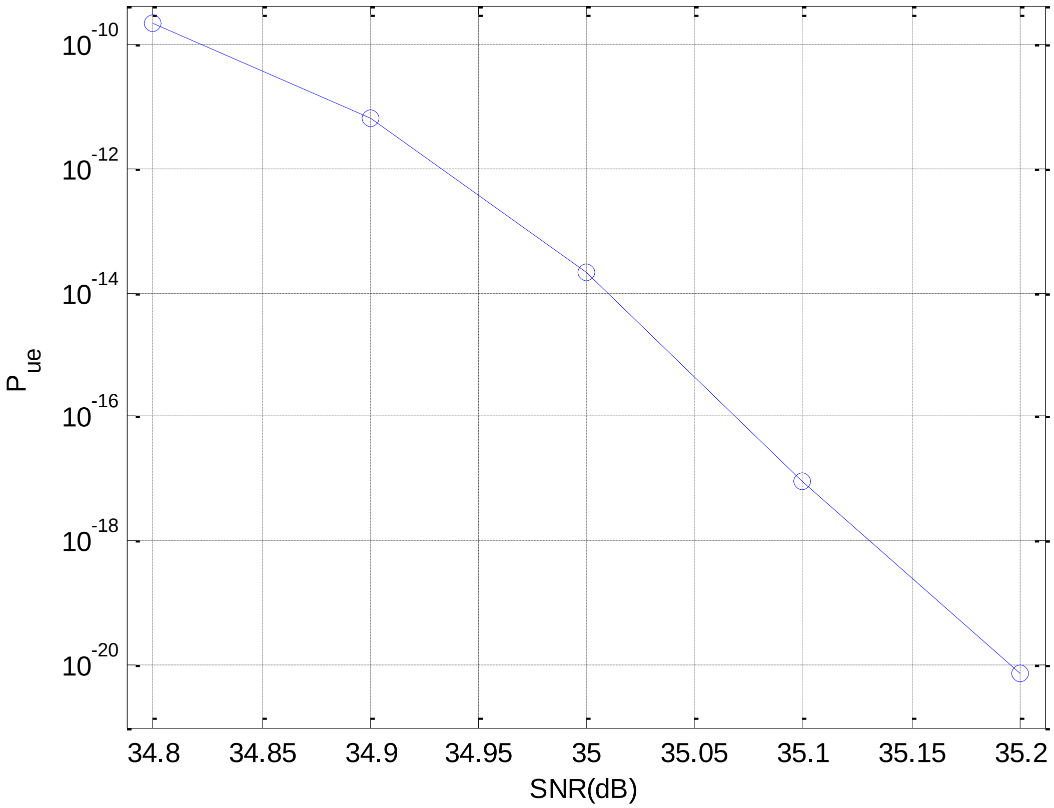
$$1 - R = 0.022222 \rightarrow \rho(R) = 0.00015792905 \Rightarrow R \le 1 - H_2(p) \text{ when } p \le 0.0001579$$

BER (bit error rate)

(after max. 30 iterations LDPC decoding)



Best P_{ue}



ON LONG SIZE UPSTREAM LDPC CODE (1024 QAM)

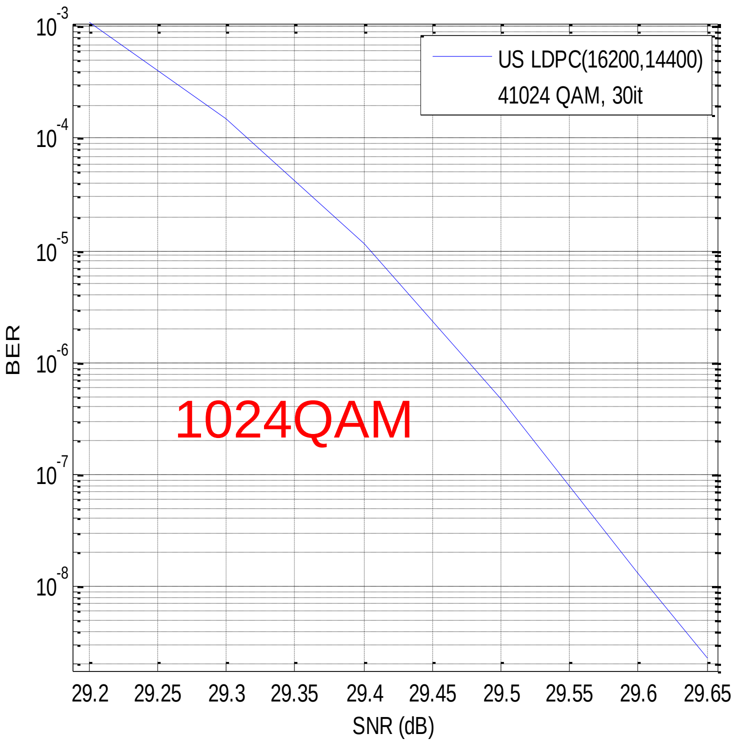
$$\text{LDPC code information}: 14400\ bits$$

$$32\ \text{bits CRC}: (n,k) = (14400,14368) \Rightarrow \text{CRC rate}: R = 0.99778$$

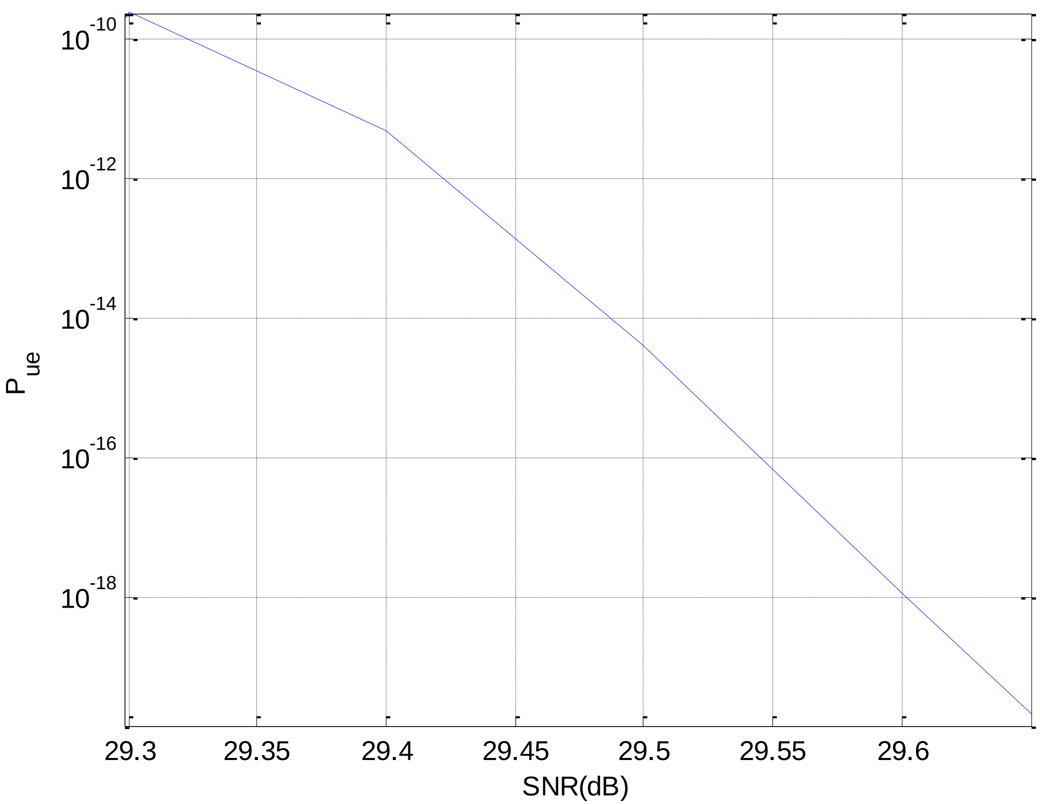
$$1 - R = 0.022222 \rightarrow \rho(R) = 0.00015792905 \Rightarrow R \le 1 - H_2(p)\ \text{when}\ p \le 0.0001579$$

BER (bit error rate)

(after max. 30 iterations LDPC decoding)



Best P_{ue}



ON MEDIAN SIZE UPSTREAM LDPC CODE (1024 QAM)

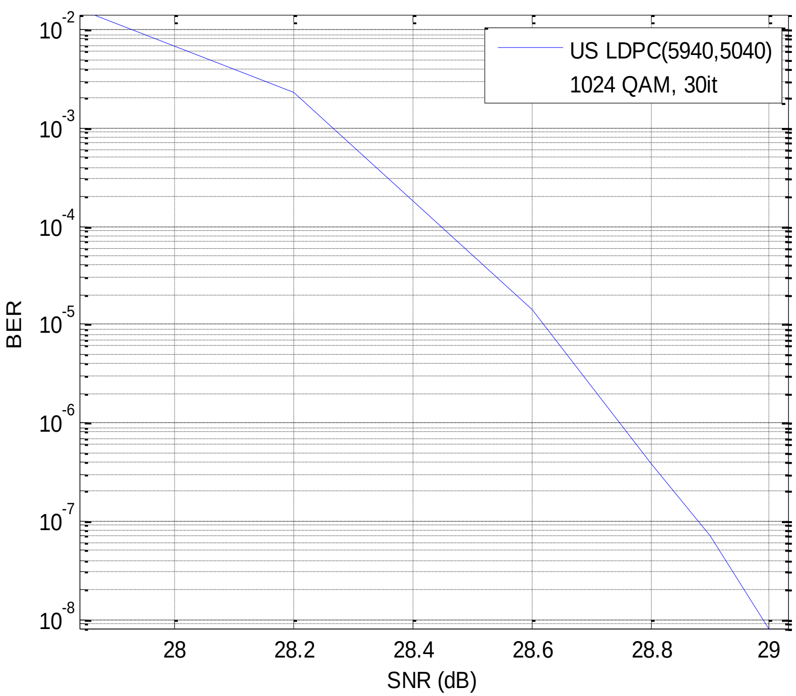
$$\text{LDPC information}: 5040\ \textit{bits}$$

$$32\ \text{bits CRC}: (n,k) = (5040,5008) \Rightarrow \text{CRC rate}: R = 0.993650793650794$$

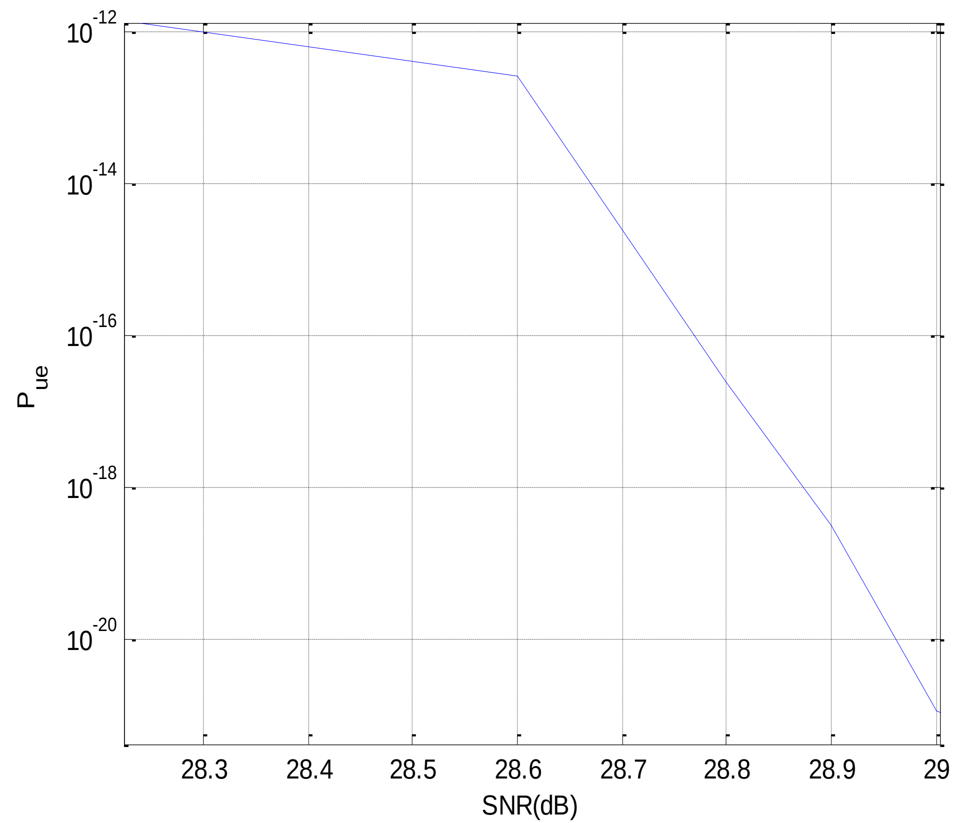
$$1 - R = 0.006349206349206 \rightarrow \rho(R) = 0.00051326018 \Rightarrow R \le 1 - H_2(p)\ \text{when}\ p \le 0.0005133$$

BER (bit error rate)

(after max. 30 iterations LDPC decoding)



Best P_{ue}



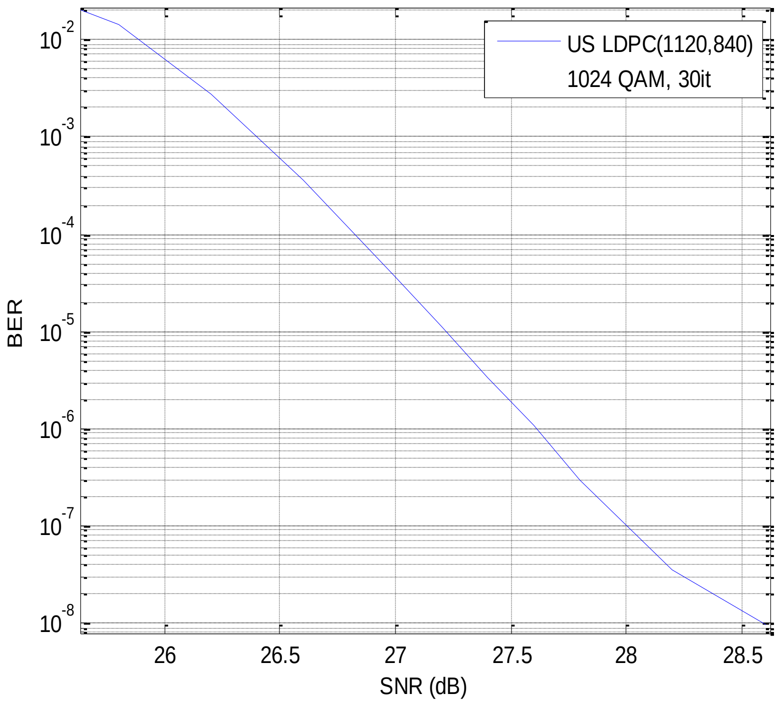
ON SHORT SIZE UPSTREAM LDPC CODE (1024 QAM)

$$\text{LDPC information code}: 840\ bits$$

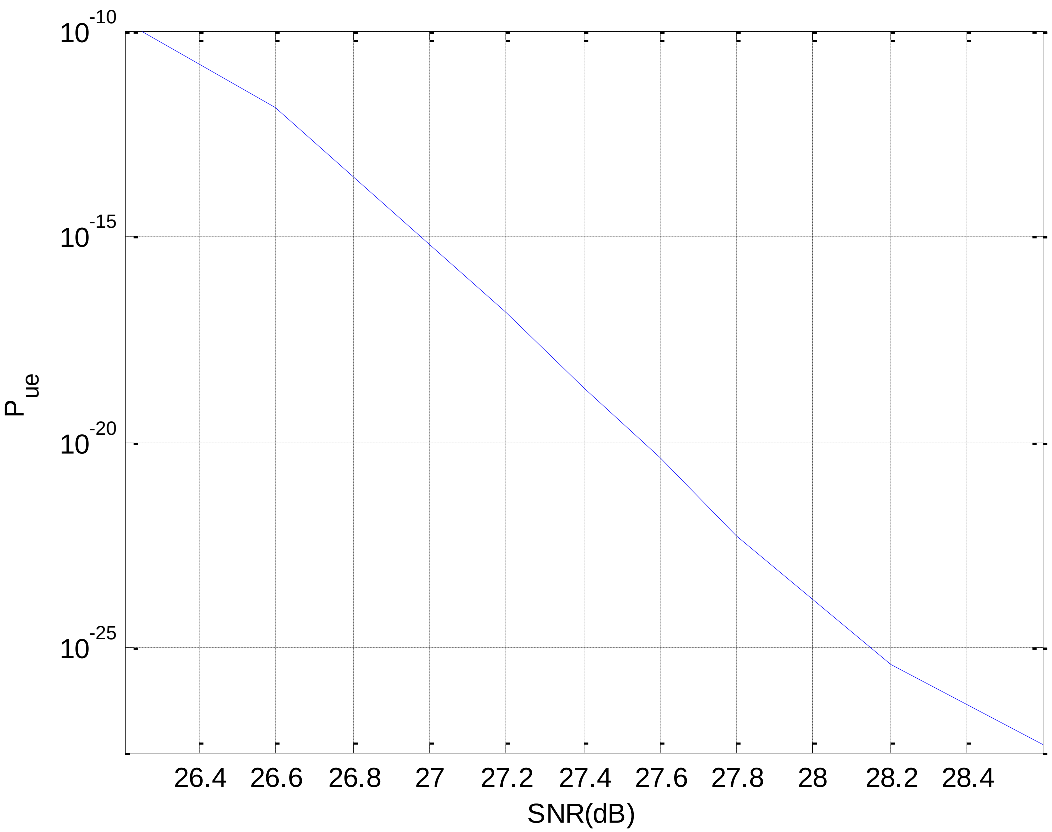
$$32\ \text{bits CRC}: (n,k) = (840,808) \Rightarrow \text{CRC rate}: R = 0.961904761904762$$

$$1-R = 0.038095238095238 \rightarrow \rho(R) = 0.004059486839 \Rightarrow R \le 1 - H_2(p)\ \text{when}\ p \le 0.004059$$

BER (bit error rate)
(after max. 30 iterations LDPC decoding)



Best P_{ue}



CONCLUSION

- **A bound for probability of an undetected error using CRC has been presented**
- **The bound is calculated for the proposed long, medium, and short codes for active plant for adding a 32 bit CRC to each codeword**
- **The overhead in adding a 32 bit CRC is only 0.2%, 0.6%, and 3.8% for the long, medium, and short size codes respectively**
- **The probability of an undetected error is less than 1e-18 above the threshold probability of error for these codes**