MCM 2015
Munich Workshop on Coding and Modulation
July 30 & 31

Efficient Most Reliable Basis decoding of short block codes

Marco Baldi
Università Politecnica delle Marche
Ancona, Italy
m.baldi@univpm.it

Outline

- Basics of ordered statistics and most reliable basis decoding
- Approaches to reduce complexity
- Hybrid decoding
- Practical code examples
- Implementation on board of spacecrafts
- Final remarks

Information Set

- Set of *k* bit positions in which any two codewords differ
- The code generator matrix **G** has linearly independent columns at those positions
- Each vector of *k* information bits can be mapped into codeword bits at those positions
- In other words, **G** can be put in reduced row echelon form with pivots on those columns

Information Set Decoding (1)

- Basic Information Set Decoding [McEliece1978]:
  - Select an information set (**at random**)
  - Put **G** in reduced row echelon form with pivots on the *k* columns corresponding to the selected information set
  - Hope that **none** of the received bits in those *k* positions are in error
  - Re-encode the received sub-vector corresponding to the information set through the generator matrix in reduced row echelon form
  - Output the recoded codeword
- If **no errors** actually occurred on the selected information set, then any error on the remaining codeword bits is corrected
- Decoding is **complete**

[McEliece1978] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory", DSN Progress Report 42-44, pp. 114-116, Jan. and Feb. 1978.

Information Set Decoding (2)

- First improved Information Set Decoding [LeeBrickell1988]:
  - Select an information set (**at random**)
  - Put **G** in reduced row echelon form with pivots on the k columns corresponding to the selected information set
  - Hope that **none or few** of the received bits in those k positions are affected by errors
  - Re-encode the information vector corresponding to the information set through the generator matrix in reduced row echelon form
    - **Try to flip all the possible combinations of 1, 2, 3, …, *i* errors affecting the received bits in the selected *k* positions and re-encode after flipping**
  - Output the recoded codeword at minimum Hamming distance from the received vector
- If ***i* or less errors** actually occurred on the selected information set, then any error on the remaining codeword bits is corrected

[LeeBrickell1988] P. Lee and E. Brickell, “An observation on the security of McEliece’s public-key cryptosystem”, Advances in Cryptology - EUROCRYPT 88, pp. 275-280, 1988.

Most Reliable Basis Decoding (1)

- In ISD, binary output channels are considered, without reliability information
- The information set is hence selected **at random**
- When reliability information is available, we can instead select the **most reliable** information set
- This reduces the probability of error over the information set bits, thus improving the decoder performance

Most Reliable Basis (MRB) decoding

or

Ordered Statistics Decoding (OSD)

Some refs

- B. G. Dorsch, “A decoding algorithm for binary block codes and J-ary output channels”, IEEE Trans. Inf. Theory, vol. 20, no. 3, pp. 391-394, May 1974.
- M. P. C. Fossorier and S. Lin, “Soft-decision decoding of linear block codes based on ordered statistics,” IEEE Trans. Inf. Theory, vol. 41, pp. 1379-1396. Sept. 1995.
- M. P. C. Fossorier and S. Lin, “Computationally efficient soft decision decoding of linear block codes based on ordered statistics,” IEEE Trans. Inf. Theory, vol. 42, pp. 738-750, May 1996.
- A. Valembois and M. Fossorier, “Box and match techniques applied to soft decision decoding,” IEEE Trans. Inf. Theory, vol. 50, no. 5, pp. 796-810, May 2004.
- H. Yagi, T. Matsushima and S. Hirasawa, “Fast algorithm for generating candidate codewords in reliability-based maximum likelihood decoding,” IEICE Trans. Fundamentals, vol. E89-A, pp. 2676-2683, Oct. 2006.
- W. Jin and M. Fossorier, “Enhanced Box and Match Algorithm for Reliability-Based Soft-Decision Decoding of Linear Block Codes,” Proc. Globecom 2006, Nov. 2006.
- Y. Wu and C. N. Hadjicostis, “Soft-decision decoding using ordered recodings on the most reliable basis,” IEEE Trans. Inf. Theory, vol. 53, no. 2, pp. 829.836, Feb. 2007.
- A. Kabat, F. Guilloud and R. Pyndiah, “New approach to order statistics decoding of long linear block codes,” Proc. Globecom 2007, pp. 1467-1471, Nov. 2007.

Most Reliable Basis Decoding (2)

- After finding the MRB, all the **Test Error Patterns (TEPs)** of 1, 2, 3, …, *i* errors are tested as in [LeeBrickell1988]
- The parameter *i* is called the **MRB order**
- Another advantage of reliability information: for each TEP we can compute a reliability metric
- **Weighted Hamming distance** = sum of the reliabilities of the bits in which the recoded codeword and the received vector differ
- It can be used:
  - to define a **quick stop** criterion
  - to **order** the TEP list (by computing it in advance through statistical arguments)
- **ML** soft-decision decoding = finding the TEP that minimizes the weighted Hamming distance (over the complete TEP list)

Most Reliable Basis Decoding (3)

1. Find the k **most reliable received bits** and collect them in a vector **v**
2. Perform **Gauss-Jordan elimination** on **G** to put it in reduced row echelon form with pivots on those k positions (if possible, otherwise slightly change the k positions, starting from the least reliable ones)
3. **Permute** the columns of **G** to obtain **G'** = [**I** | **P**]
4. **Re-encode** **v** by **G'** to obtain the first candidate codeword **c** = **v** **G'**
5. Consider all (or an appropriate subset of) **TEPs** of length k and Hamming weight $w \leq i$ and, for each of them:
   1. Add it to **v** and encode by **G'**
   2. Compute the weighted Hamming distance from the received vector
   3. If the distance is smaller than that of the previous candidate codeword, then update the candidate, otherwise keep the candidate unchanged
6. Output the candidate codeword as the decoded codeword

Most Reliable Basis Decoding (4)

- Given the MRB order i, the number of TEPs to test is

$$N_{\text{TEP}} = \sum_{j=0}^{i} \binom{k}{j}$$

- If $i = k$, MRB decoding = ML decoding, $N_{\text{TEP}} = 2^k$ (optimal performance but huge complexity)
- Decrease i to get worse performance but acceptable complexity
- To avoid decreasing i too much, we can:
  - **optimize algorithms** (e.g., reusing previous candidate codewords to compute new ones)
  - reduce the average value of N_{TEP} by **thresholding** the weighted Hamming distance
  - **selectively invoke** the MRB decoder (only after a failed lighter decoding attempt) → hybrid decoding

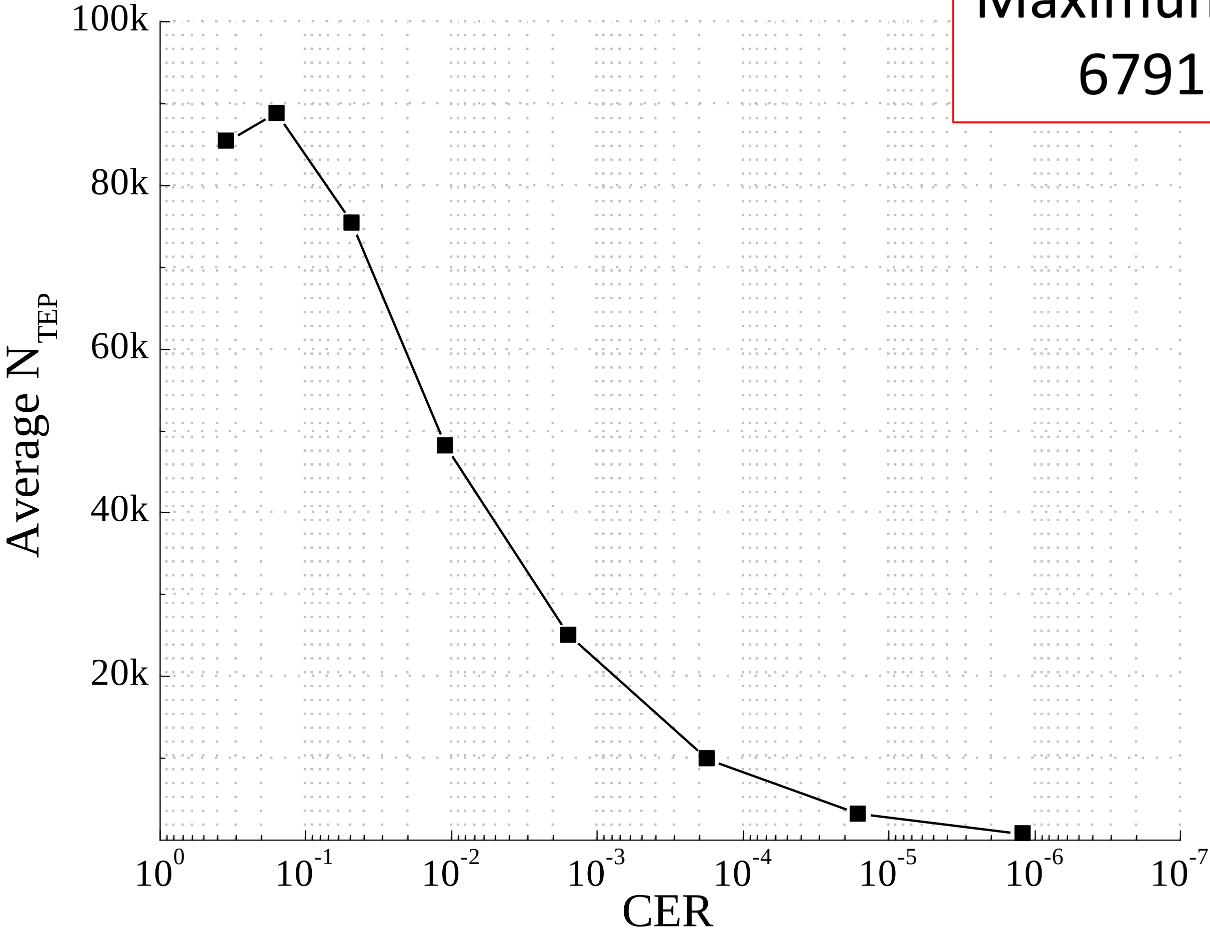
Reduction of N_{TEP} (1)

- A first step consists in **ordering the TEP list**
- On average (and for sufficiently high SNR), an EP with weight w is more probable than one with weight $w + 1$
- However, some specific EPs with weight $w + 1$ may be more probable than others with weight w
- They can be found *a priori* by considering the **average reliabilities** of the bits in the MRB
- After having ordered the TEP list, the weighted Hamming distance can be compared with some **threshold**
- If it goes below the threshold, we can avoid considering other TEPs and output the current candidate codeword

Reduction of N_{TEP} (2)

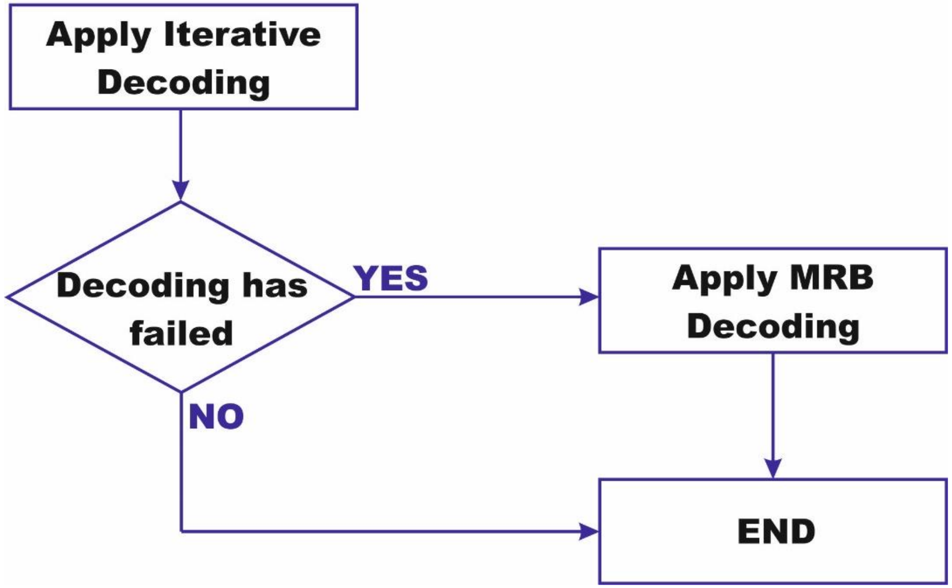
- Binary LDPC code, n = 128, k = 64, i = 4

Maximum N_{TEP}: 679121



Hybrid MRB Decoding

- For codes allowing some form of **low complexity decoding** (like iterative algorithms (IAs): SPA for LDPC codes, BCJR for Turbo codes, …)
- Invoke the MRB decoder only when the IA fails
- MRB uses the soft information **from the channel** (not from the IA)



[Baldi2014] M. Baldi, F. Chiaraluce, N. Maturo, G. Liva and E. Paolini, “A Hybrid Decoding Scheme for Short Non-Binary LDPC Codes”, IEEE Comms. Letts. Vol. 18, No. 12, pp. 2093-2096, 2014.

[Baldi2015] M. Baldi, N. Maturo, F. Chiaraluce, E. Paolini, “On the applicability of the most reliable basis algorithm for LDPC decoding in telecommand links”, Proc. ICICS 2015, Amman, Jordan, Apr. 2015.

Complexity (1)

- We can count the number of **binary operations** required per each decoded codeword
- Basic routines:
  - Ordering of n real values
  - Processing the $k \times n$ matrix **G** to obtain **G'**
  - Perform a vector-matrix product
  - Consider N_{TEP} TEPs and compute the relevant metrics
- We consider q quantization bits for real variables

$$\boxed{C_{\mathrm{MRB}} = qn\log_2 n + \left(\frac{k}{2}\right)^3 + N_{\mathrm{TEP}}\left(2qi + q\frac{n-k}{2} + \frac{nk}{2}\right)}$$

Complexity (2)

- For the Hybrid decoder: $\boxed{C_{\text{Hybrid}} = C_{\text{IA}} + \alpha C_{\text{MRB}}}$

with α = detected CER of the IA, and

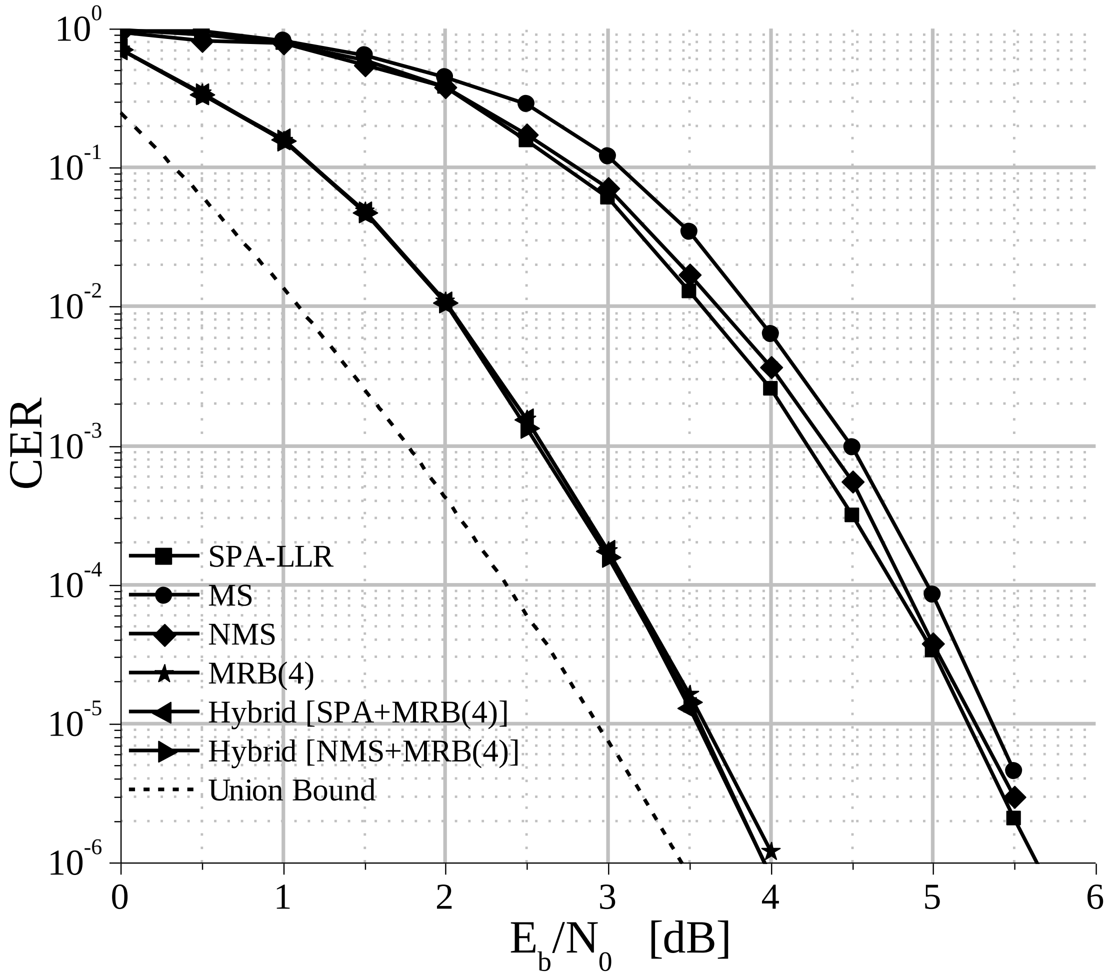
$$\left.\begin{aligned}
C_{\text{SPA}} &= I_{\text{ave}} n \left[q\left(8d_v + 12R_c - 11\right) + d_v \right] \\
C_{\text{MS}} &= I_{\text{ave}} n \left[q\left(3d_v + 2R_c\right) + 2d_v - 1 + R_c \right] \\
C_{\text{NMS}} &= C_{\text{MS}} + I_{\text{ave}} n \left(2d_v + 1\right)
\end{aligned}\right\} \text{IA Complexity}$$

I_{ave} = average number of iterations of the IA

d_v = average column weight of **H**

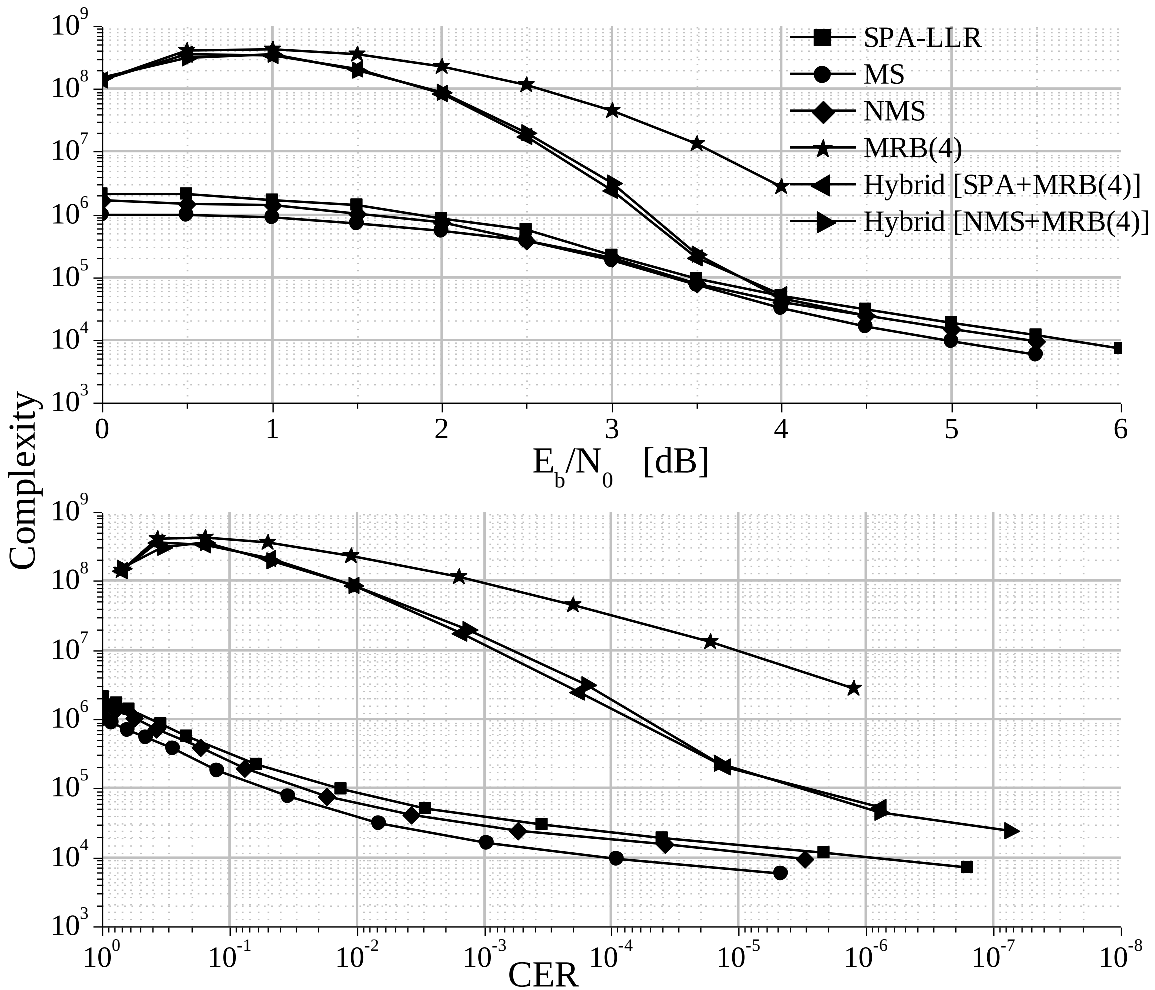
Example: $LDPC_2(128, 64)$

- Protograph-based binary LDPC code
- Under consideration for **CCSDS TC recommendations**
- Gain over IA alone: ≈ **1.6 dB** @ CER = 10^{-5}



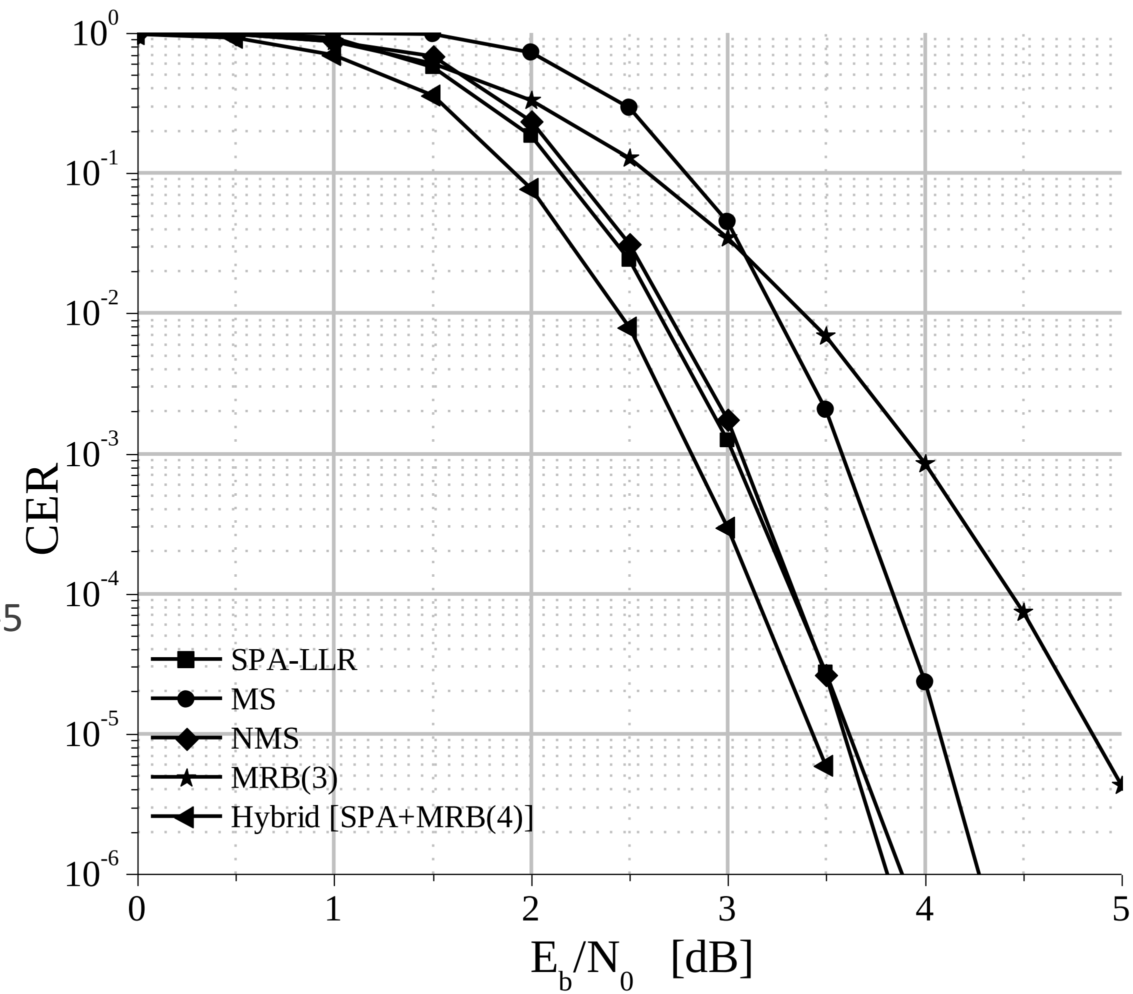
Example: $LDPC_2(128, 64)$ (2)

- Number of binary operations per decoded codeword
- q = 6 bits for quantization
- @ CER = 10^{-5}: hybrid decoding has **10x** complexity than IA alone



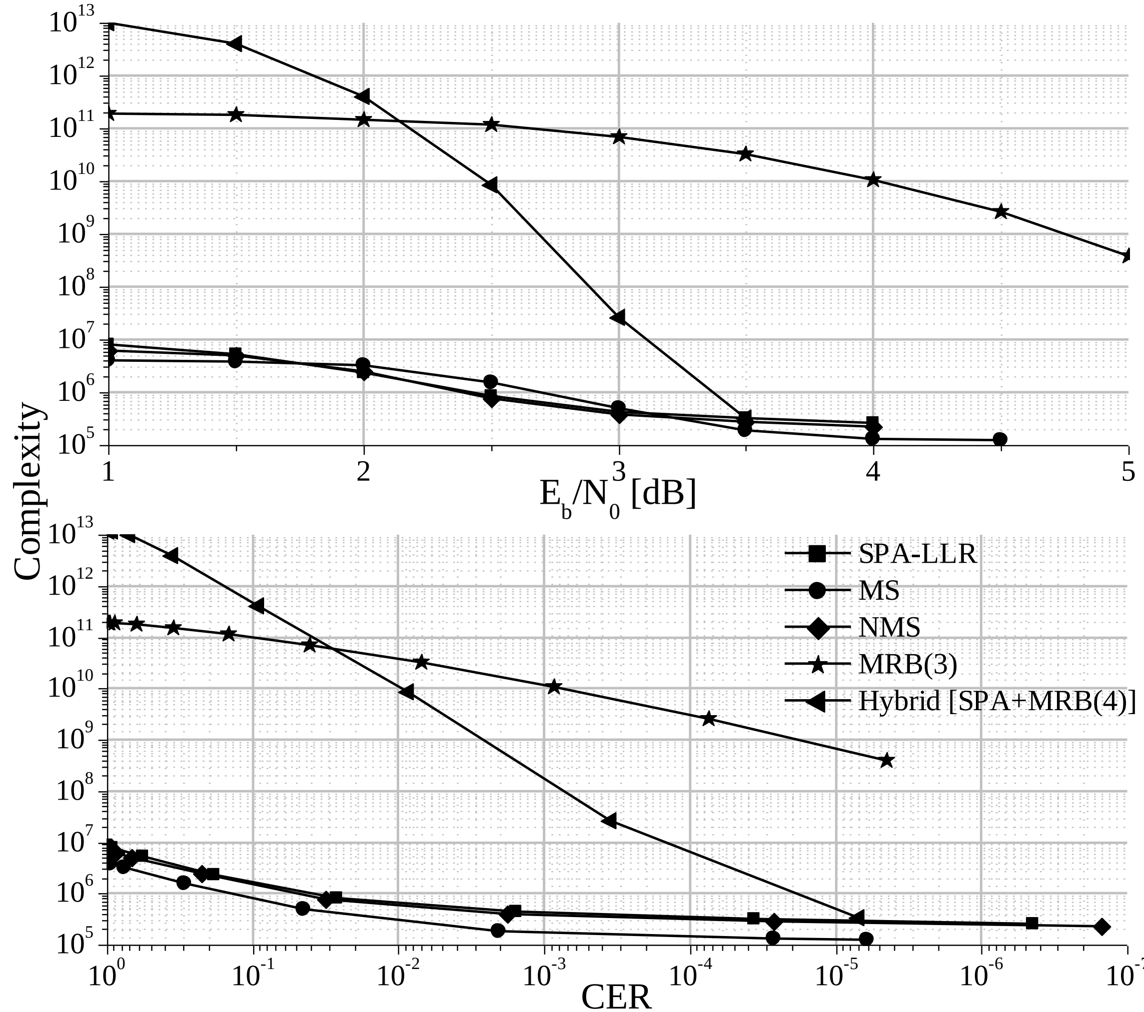
Example: $LDPC_2(512, 256)$

- Protograph-based binary LDPC code
- Under consideration for **CCSDS TC recommendations**
- Gain over IA alone: ≈ **0.15 dB** @ CER = 10^{-5}



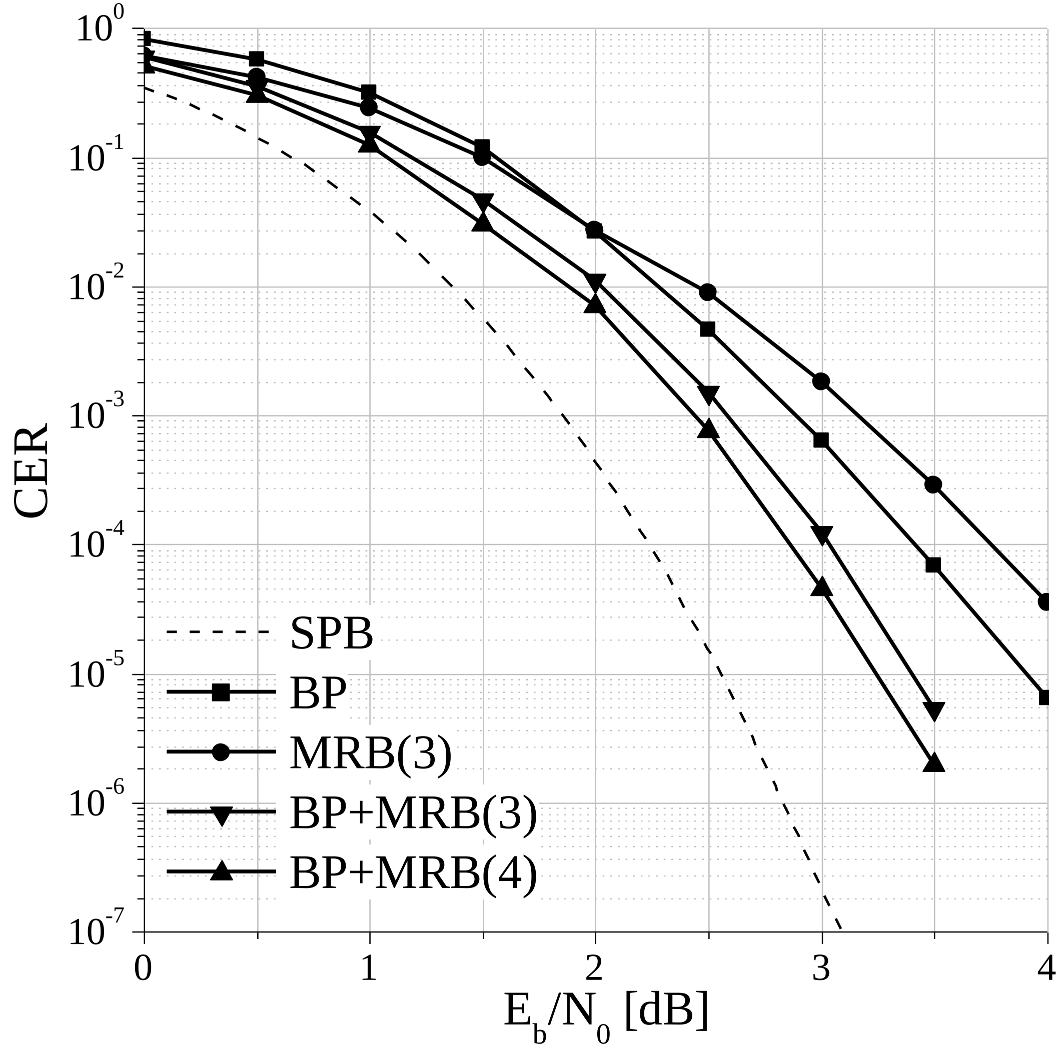
Example: $LDPC_2(512, 256)$ (2)

- Number of binary operations per decoded codeword
- 6 bits for quantization
- @ CER = 10^{-5}: hybrid decoding has almost the **same complexity** than IA alone



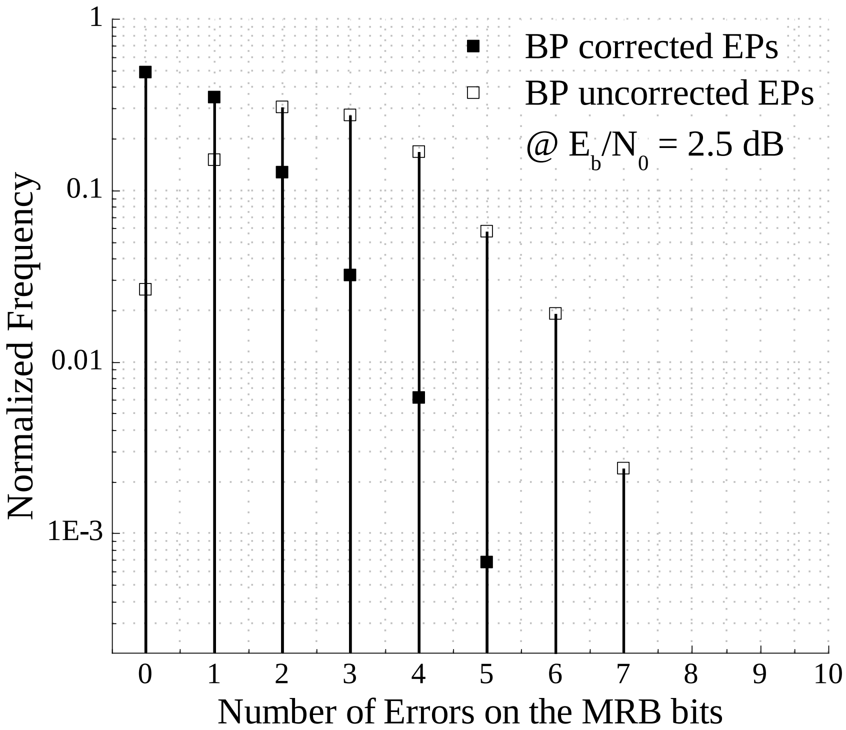
Example: $\text{LDPC}_{64}(32, 16)$ (1)

- Non-binary LDPC code with $d_v = 2$
- Gain over IA alone ($i = 3$): ≈ **0.5 dB** @ CER = 10^{-5}
- Gain over IA alone ($i = 4$): ≈ **0.7 dB** @ CER = 10^{-5}
- Gain over MRB alone ($i = 3$): ≈ **0.75 dB** @ CER = 10^{-4}



Example: $\text{LDPC}_{64}(32, 16)$ (2)

- How can the hybrid decoder **improve over both** IA and MRB used alone?
- The IA is not a bounded-distance decoder, therefore:
  - it may succeed on vectors at a **large Euclidean distance** from the BPSK-modulated transmitted codeword
  - it may fail on vectors at a **small Euclidean distance** from it
- The MRB decoder corrects all error patterns with $w \le i$ errors on the MRB bits



NEXCODE Project

- Title: **Next Generation Uplink Coding Techniques** (NEXCODE)
- Funding entity: **European Space Agency** (ESA/ESTEC)
- Aims:
  - Designing and implementing error correcting coding techniques for the new **telecommand standard** for near Earth and deep space missions
  - Assessing their impact on the overall TT&C transponder architecture
- Partners:
  - DEIMOS Engenharia (Portugal – Spain)
  - CNIT (University of Bologna, Polytechnic of Turin, Polytechnic University of Marche), Italy
  - CTTC, Spain
  - Thales Alenia Space, Italy

MRB decoding in the Space (1)

- **On-Board Computer (OBC)** hardware configuration (from TAS-I ASIC Processor LEON2-FT second generation used in the JUNO Mission Ka-Band Transponder):
  - Clock Frequency: **100 MHz**
  - Data Cache: **4Kb**
  - **8 bit** bus
  - NO FPU
  - NO optimized Integer Unit

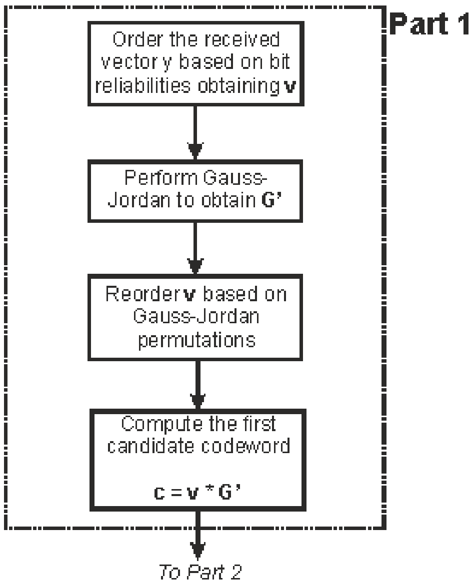
- Emulation of the OBC hardware configuration on a Virtex-6 XC6VLX240T-1FFG1156 FPGA
- Estimation of the latency due to MRB decoding if a **full software** (C++) implementation is used
- Focus on the $LDPC_2(128, 64)$ code

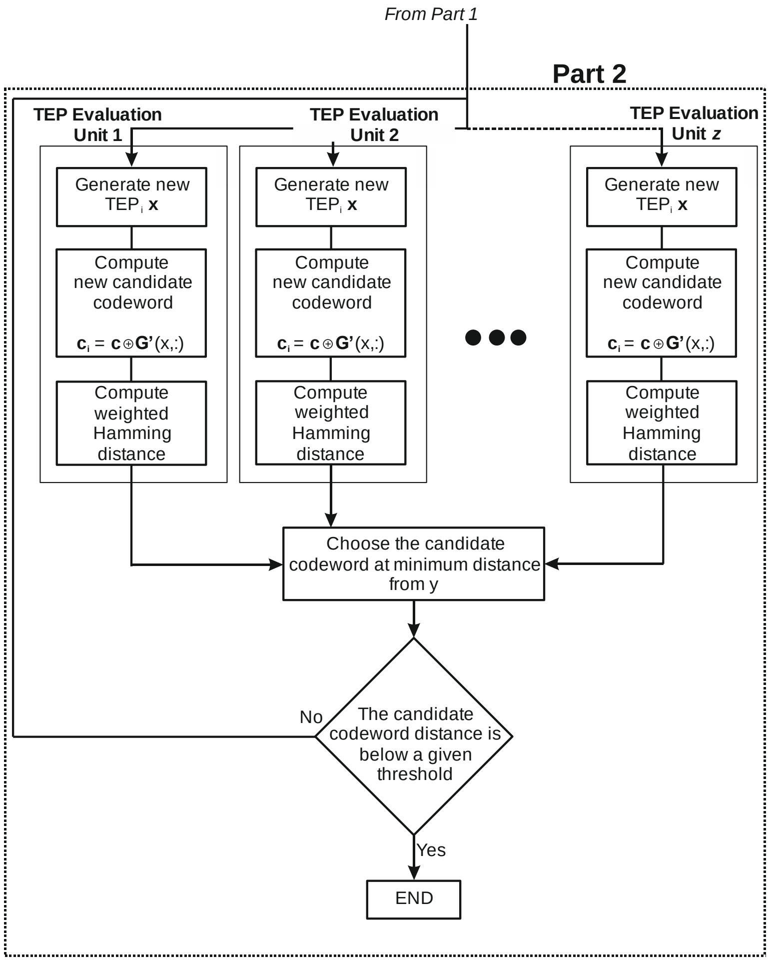
MRB decoding in the Space (2)

- To evaluate 1 TEP, the OBC needs **0.0208 s**
- 200K TEPs are necessary to ensure satisfactory performance in the worst case (much less on average)
- Worst case latency = 4160 s > 69 min → **unacceptable**
- Considering a 2 s latency as acceptable in the deep space scenario, we can use at most 100 TEPs
- With 100 TEPs only, the CER performance is worse than that of the sole NMS decoder → **unacceptable**
- A "mixed" implementation (**software + hardware**) is required

MRB decoding in the Space (3)

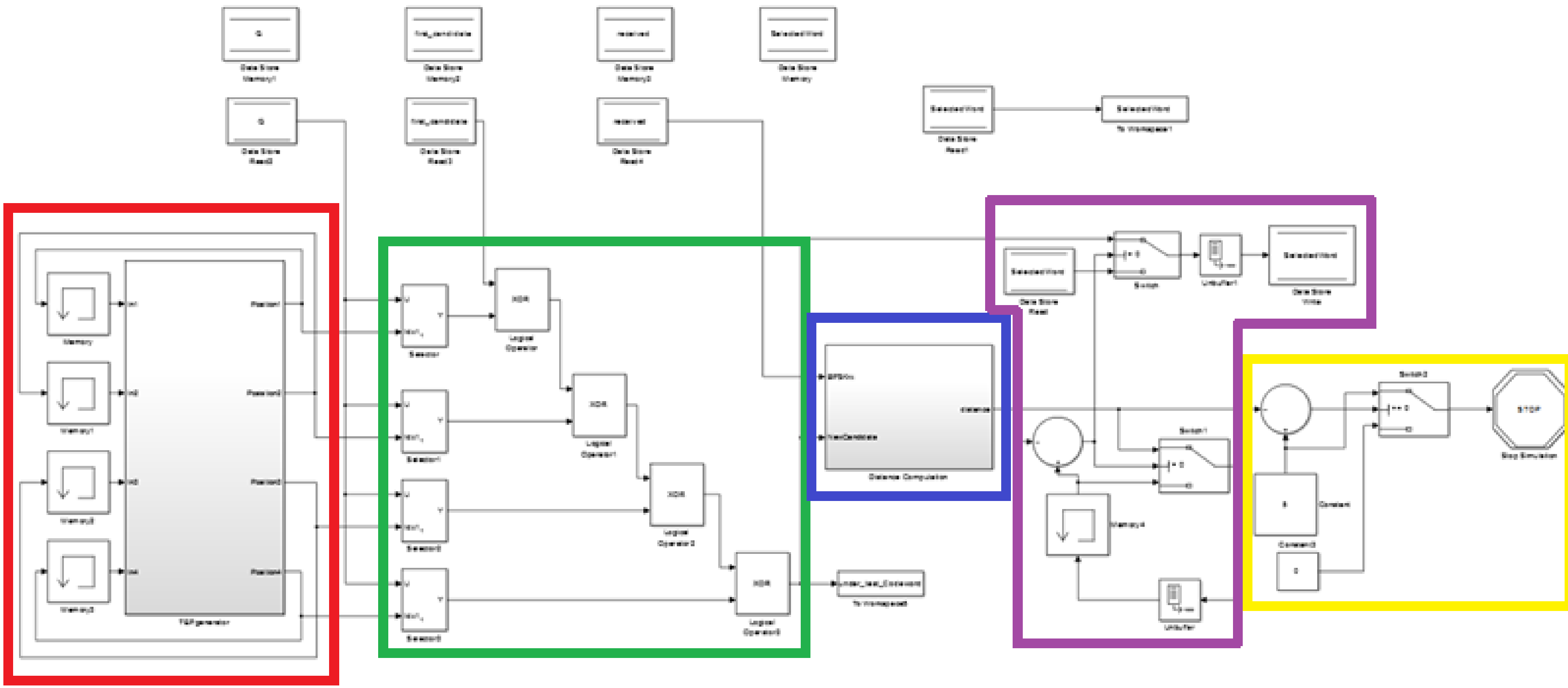
- Decomposition of the MRB decoding algorithm in two parts
- Part 2 is more suitable for HW implementation





TEP Evaluation Unit Simulink Model

- Work in Progress… (thanks to **Deimos** and **Nicola Maturo**)



Parallel Implementation of MRB

- Worst-case latency (s) with 200k TEPs:

200000 TEPs	f_{clock} = 1 MHz	f_{clock} = 10 MHz	f_{clock} = 100 MHz	f_{clock} = 1 GHz
N_{Teu} = 1	840.0333891	84.00333891	8.400333891	0.840033389
N_{Teu} = 10	84.03338906	8.403338906	0.840333891	0.084033389
N_{Teu} = 100	8.43338906	0.843338906	**0.084333891**	0.008433389
N_{Teu} = 1000	0.87338906	0.087338906	0.008733891	$8.73 \cdot 10^{-4}$
N_{Teu} = 10000	0.11738906	0.011738906	0.001173891	$1.17 \cdot 10^{-4}$

- By exploiting its intrinsic parallelism, MRB decoding can become **feasible** even **on board of spacecrafts**

Hints for future work

- The original MRB/OSD stems from the ISD in [LeeBrickell1988]
- Further advances in ISD [Stern1989, Canteaut1998] have been exploited to trade time complexity for space complexity through the “Box and Match” algorithm [Valembois2004]
- Recently, ISD has been improved again [Becker2012]
- Could these improvements be reflected into MRB/OSD?

[Stern1989] J. Stern, “A method for finding codewords of small weight,” in Coding Theory and Applications, G. Cohen and J.Wolfmann, Eds. New York: Springer-Verlag, 1989, pp. 106–113.

[Canteaut1998] A. Canteaut and F. Chabaud, “A new algorithm for finding minimum weight words in a linear code: Application to McEliece’s cryptosystem and to narrow-sense BCH codes of length 511,” IEEE Trans. Inform. Theory, vol. 44, pp. 367–378, Jan. 1998.

[Becker2012] A. Becker, A. Joux, A. May and A. Meurer, “Decoding random binary linear codes in $2^{n/20}$: How 1 + 1 = 0 improves information set decoding,” Proc. EUROCRYPT 2012, vol. 7237 of Lecture Notes in Computer Science, pp. 520–536, Springer-Verlag, 2012.