Algorithmic Optimization of Non-Binary Decoders.

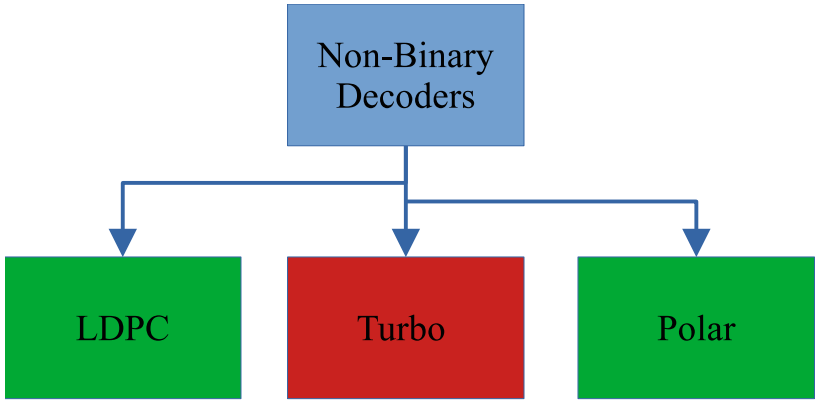
Joseph JABOUR

Thesis Defense held in Lorient on 14 Dec, 2023.

Rapporteurs:	Francisco GARCÍA HERRERO	Professeur à Universidad Complutense de Madrid.
	Christophe JEGO	Professeur à ENSEIRB-MATMECA - IMS
Examinateurs :	Catherine DOUILLARD	Professeure à l'IMT Atlantique
	Charly POUILLAT	Professeur à INP-ENSEEIHT
Dir. de thèse :	Emmanuel BOUTILLON	Professeur à l'Université Bretagne Sud
Encadrants de thèse :	Ali ALGHOUWAYEL	Maître de Conférences à l'IMT Atlantique
	Hussein HIJAZI	Maître de Conférences à Lebanese International University
	Cédric MARCHAND	Docteur-Ingénieur de recherche à l'Université Bretagne Sud

Brief Context and Objective

- This thesis is a part of the Quasi Cyclic Small Packet (QCSP)[1] project.
- QCSP Project: Association of non-binary codes with Cyclic-Code Shift Keying (CCSK)[2] for self-synchronization and identification waveforms for IoT networks.
- CCSK is a low-rate non-binary modulation of rate $r = \frac{\log_2(q)}{q}$ where q is field order.
- Thesis role: investigates non-binary decoders and aims to optimize their decoding algorithms.



[1] K. Saied. (2019), "Quasi Cyclic Small Packet," [Online]. Available: https://qcsp.univ-ubs.fr.

[2] G. Dillard, M. Reuter, J. Zeiddler, *et al.*, "Cyclic Code-Shift Keying: A Low Probability of Intercept Communication Technique." *IEEE Transactions on Aerospace and Electronic Systems*.

Error Control Codes I

- Shannon[3] proved that reliable communication is possible.
- Since then, plenty of error correction codes have been proposed.
- In general, an error correction code receives an information block of length K and encodes it to generate a codeword of length N by introducing $M = N - K$ redundant symbols.

Error Control Codes II

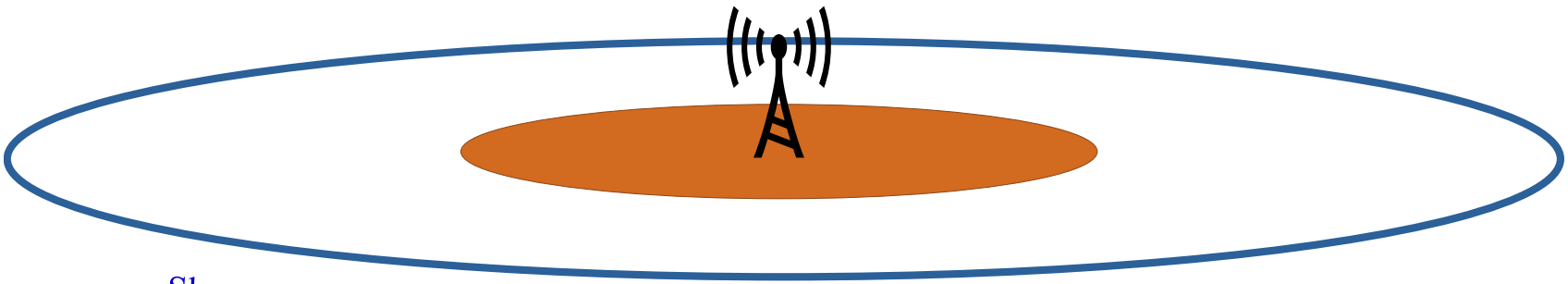


Figure 1: Performance of classical codes (before 1993).

Error Control Codes III

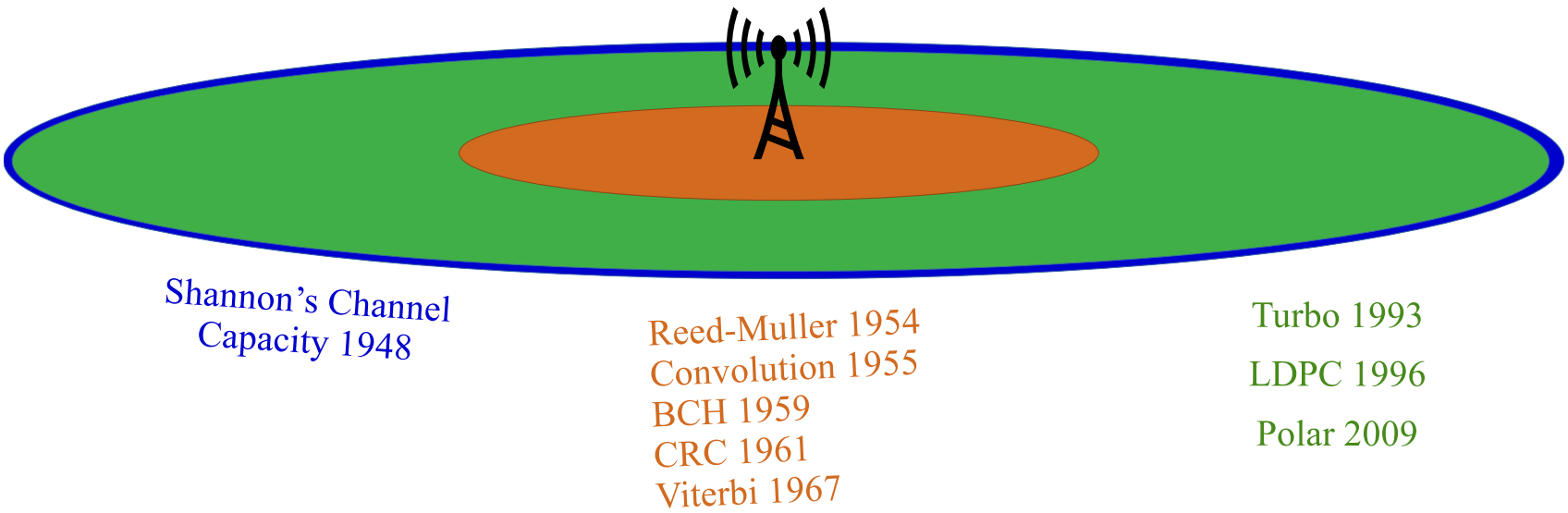


Figure 2: Performance of capacity-approaching codes

[3] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

If all is good, why non-binary codes?

- Performance of binary codes degrades under:
  - Short packet communication.
  - Non-binary Modulation.
- Solution: Use NB codes.

Performance of Binary Vs. NB LDPC

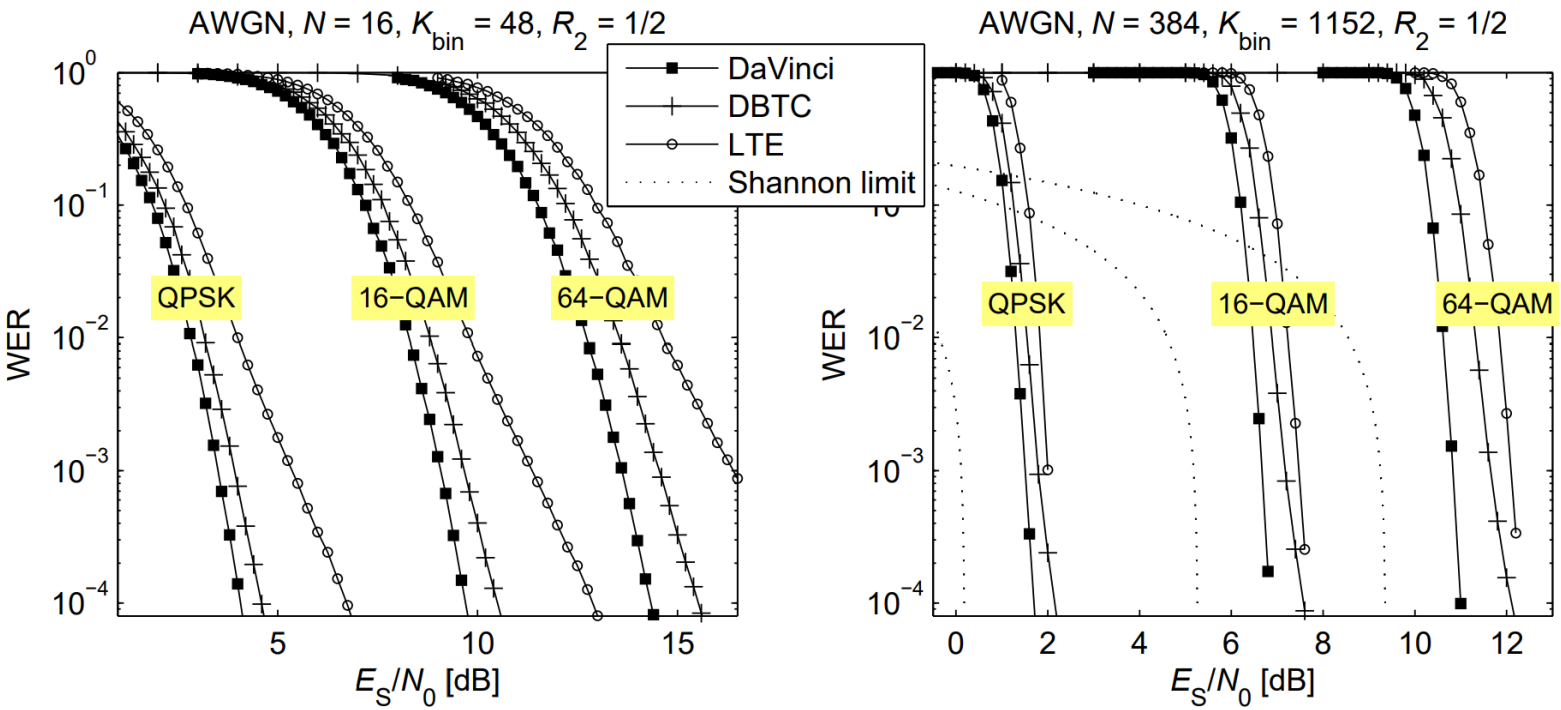
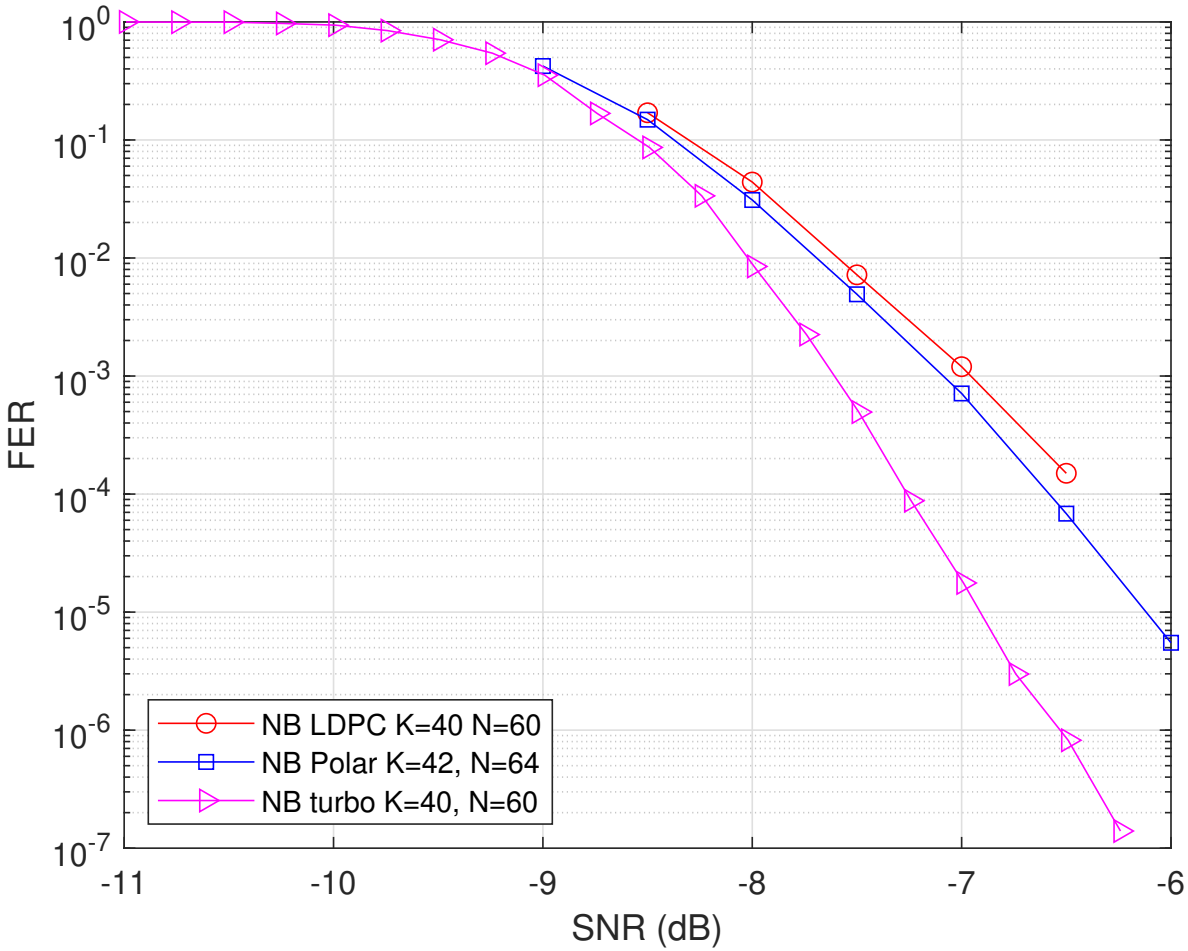


Figure 3: Binary vs. Non-Binary GF(64) LDPC over Different Modulation Schemes[4]

[4] S. P. et al., "Performance evaluation of non-binary ldpc codes on wireless channels," in *ICT-MobileSummit 2009 Conference Proceedings*, 2009, ISBN: 978-1-905824-12-0.

Performance of Non-Binary Codes on CCSK Modulation

- $r = \frac{Kp}{Nq}$.



Alright! Let's use non-binary codes.

- HIGH COMPLEXITY DECODERS.
- However, standardized for the Chinese Satellite Navigation System , BeiDou[5] for low code rate applications.

[5] C. S. N. Office. (2019), "BeiDou Navigation Satellite System Signal In Space Interface Control Document," [Online]. Available: http://www.beidou.gov.cn/xt/gfxz/201912/P020230516558050038035.pdf

Binary Vs. Non-Binary Codes

- Binary Codes have symbols and coefficients defined on GF($q = 2^p$) with $p = 1$.
- Non-Binary Codes have symbols and coefficients defined on GF($q = 2^p$) with $p > 1$.
- Increases complexity of arithmetic operations.

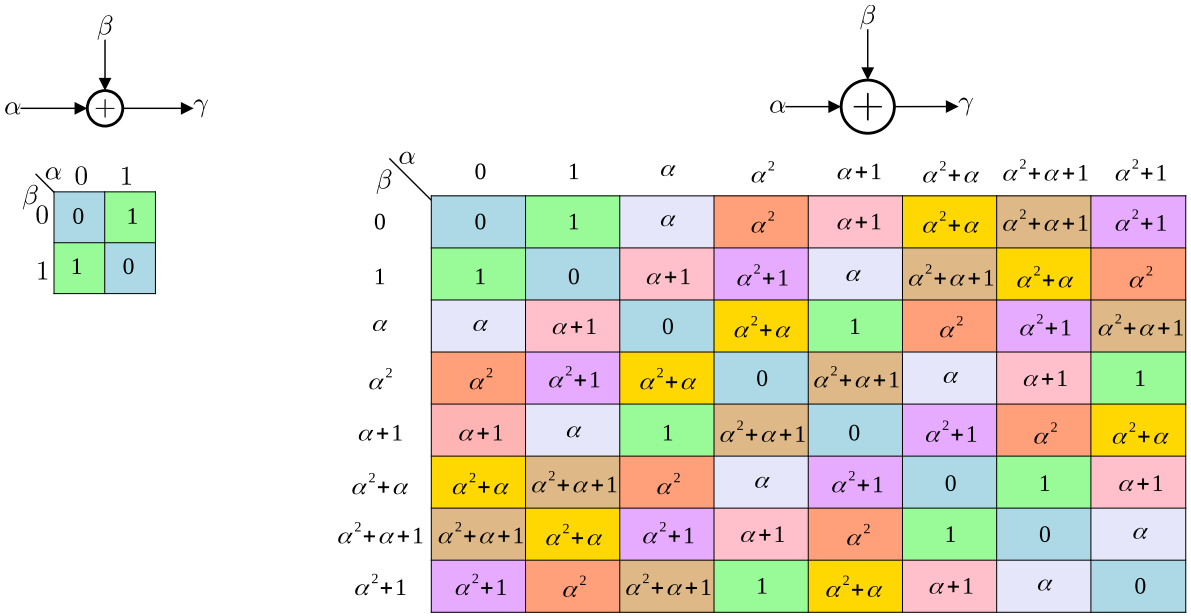


Figure 4: Arithmetic Operations on GF(2) and GF(8).

Non-Binary LDPC Codes

Structure of NB-LDPC Codes

- LDPC Codes invented by R. Gallager in 1960[6].
- Rediscovered by D. Mackay in 1996[7,8].
- Linear block code defined by sparse Parity Check Matrix (PCM) **H** of dimension $M \times N$ over a Galois field GF$(q = 2^p)$ with $p > 1$.
  - M: Size of redundant symbols.
  - N: Size of codeword.
- Codeword X is valid iff $X \cdot \mathbf{H}^T = 0$ where $\mathbf{H}^T$ is the transpose of **H**.

[6] R. Gallager, *Low Density Parity-Check Codes*. Cambridge MA: MIT Press, 1963.

[7] D. MacKay, "Near shannon limit performance of low density parity check codes," English, *Electronics Letters*, vol. 32, 1645–1646(1), 18 Aug. 1996, ISSN: 0013-5194. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/el_19961141.

[8] D. MacKay, "Good error-correcting codes based on very sparse matrices," in *Proceedings of IEEE International Symposium on Information Theory*, 1997, pp. 113–. DOI: 10.1109/ISIT.1997.613028.

Structure of NB-LDPC Decoder

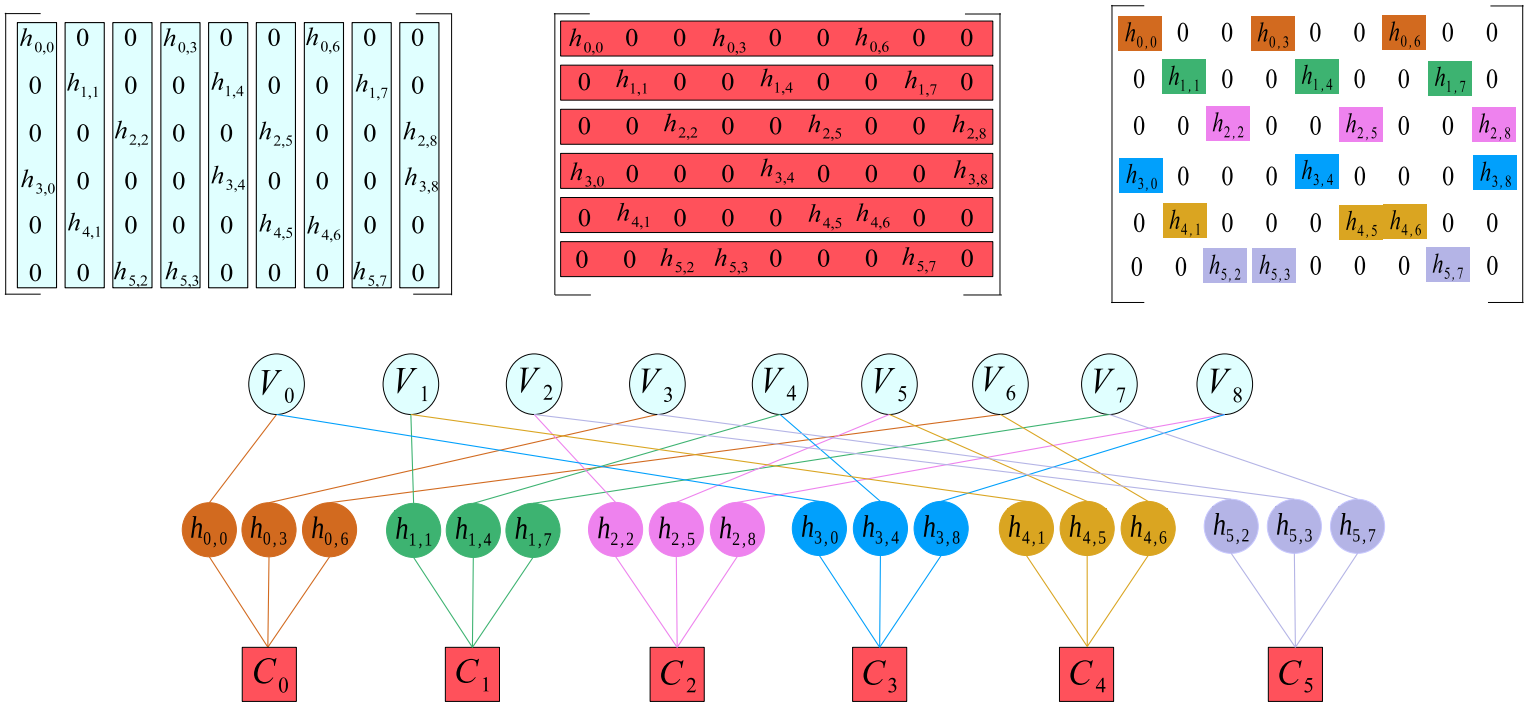


Figure 5: LDPC Decoder for $N = 9$ and $K = 3$.

- $d_v = 2$ have good performance and more hardware friendly[9].

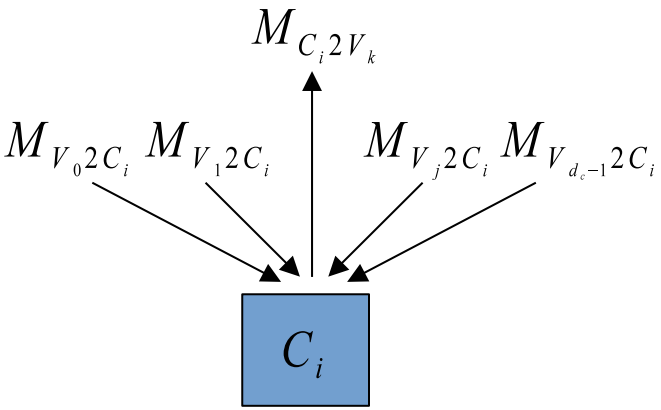
[9] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular (2,d$_c$)-LDPC codes over GF(q) using their binary images," *IEEE Transactions on Communications*, vol. 56, no. 10, pp. 1626–1635, 2008. DOI: 10.1109/TCOMM.2008.060527.

Min-Sum Algorithm

- Sub-optimal algorithm that introduces mathematical approximation to reduce the processing complexity.
- Exchanged (q-ary) messages defined as Log-Likelihood Ratios (LLRs).

$$M_{V_j 2 C_i} = [15, 0, 7, 4, 5, 1, 27, 2]$$

Most reliable symbol: α^0 Least reliable symbol: α^5



$$M_{C_i 2 V_k}[\alpha] \approx \min_{\substack{\sum_{j \neq k} \\ h_{i,j} \neq 0}} \Big\{ \sum_{\substack{j \neq k \\ h_{i,j} \neq 0}} M_{V_j 2 C_i}[\alpha_j] \Big\} \quad (1)$$

Forward-Backward Approach

Complexity: $d_c \; q^{d_c - 1}$.

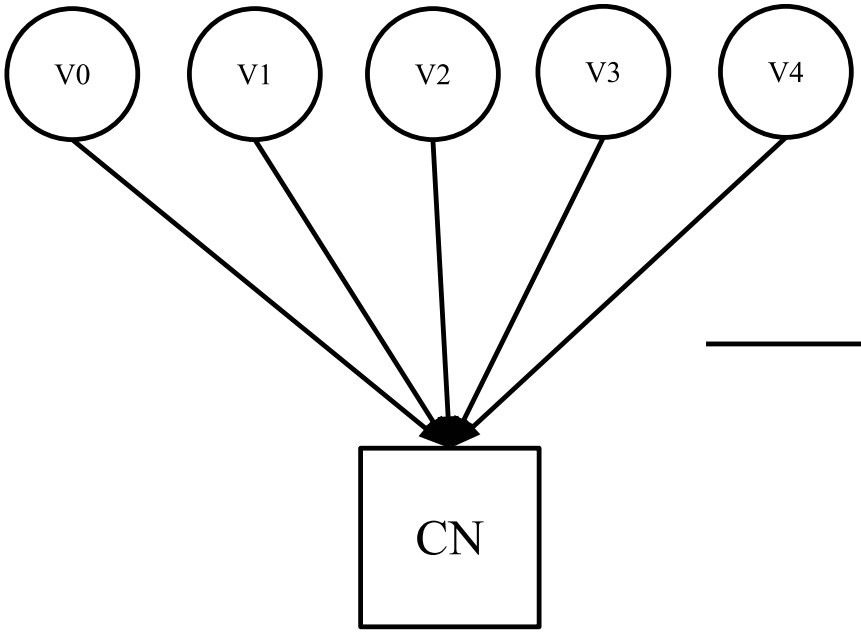


Figure 6: Conventional Check Node for $d_c = 5$.

Complexity: $3(d_c - 2)q^2$.

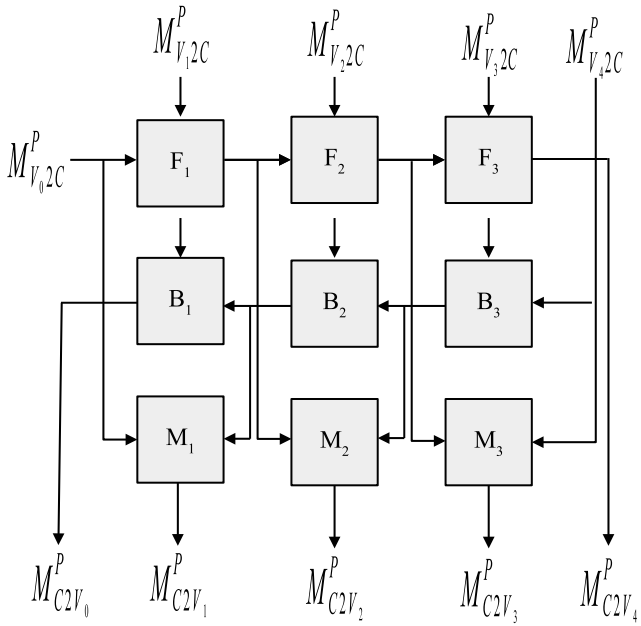


Figure 7: Check Node Decomposition for $d_c = 5$.

Min-Sum Approximation I

Let $A = [5, 4, 6, 8, 1, 7, 3, 0]$ and $B = [8, 2, 0, 9, 5, 2, 7, 6]$.

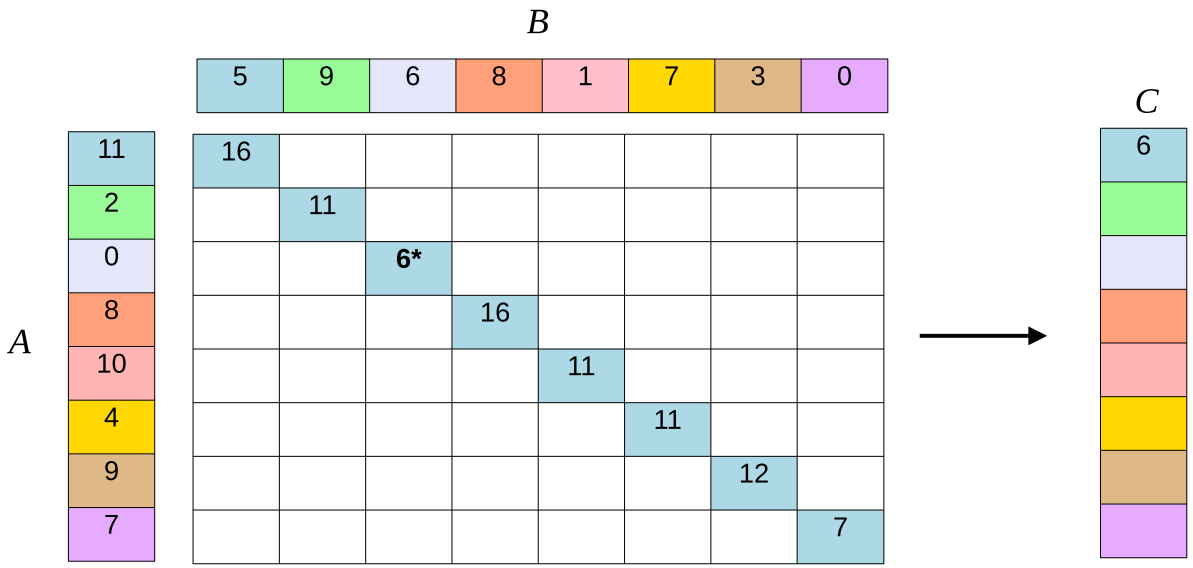


Figure 8: Toy Example on GF(8) for Check Node Processing over Min-Sum.

Min-Sum Approximation II

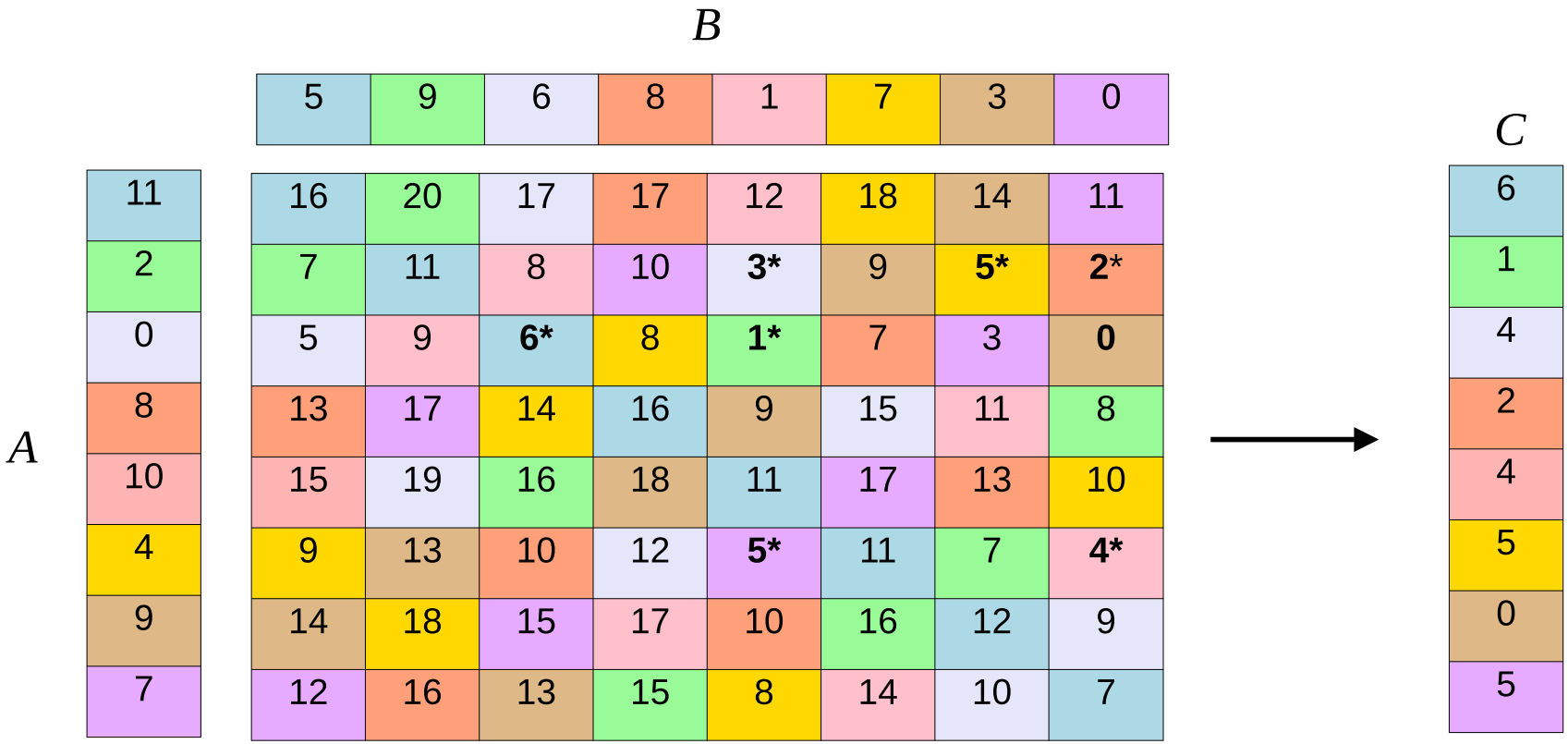


Figure 9: Toy Example on GF(8) for Check Node Processing over Min-Sum.

Min-Sum Approximation III

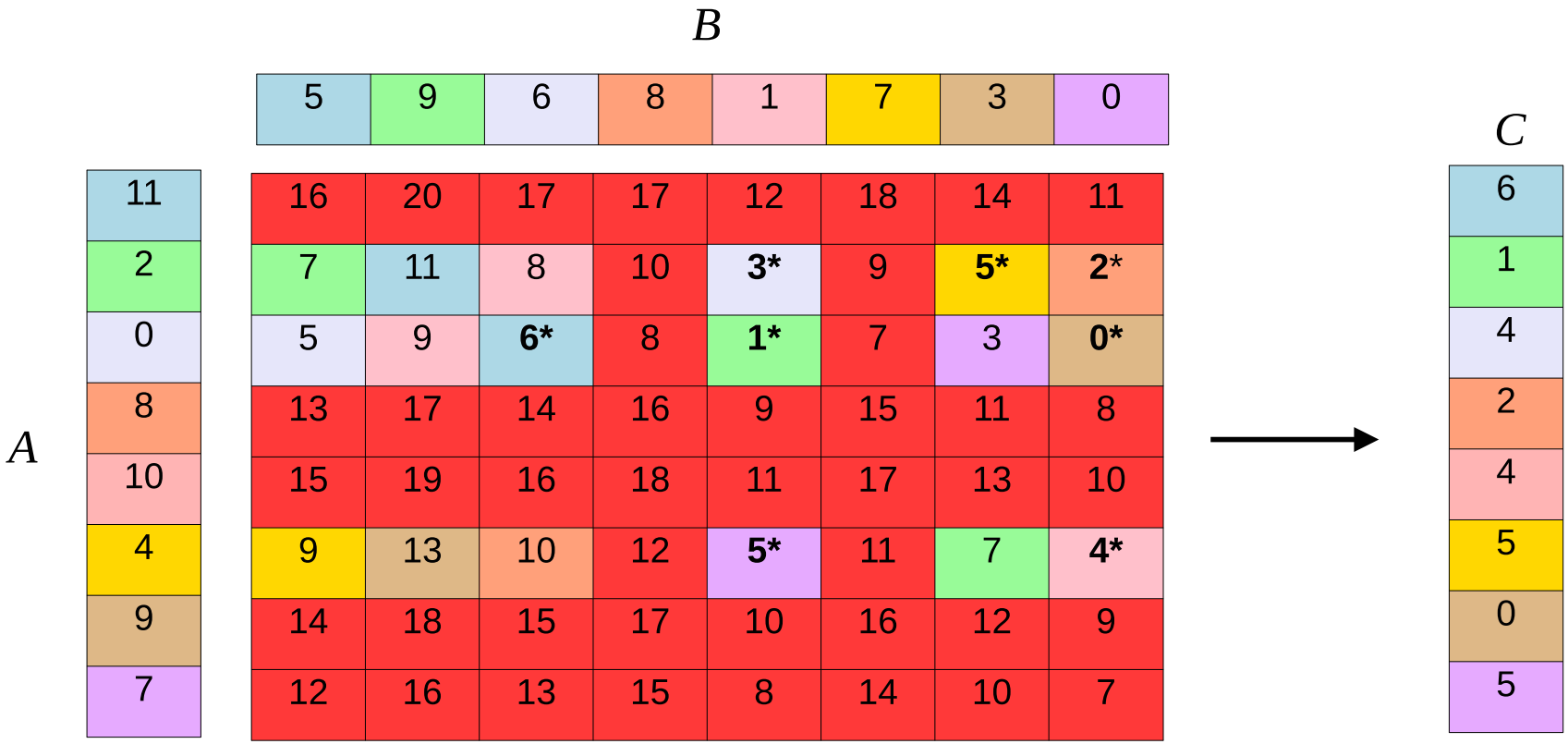


Figure 10: Toy Example on GF(8) for Check Node Processing over Min-Sum.

Extended Min-Sum Algorithm I

When sorting the MS messages, the sorted messages are
$A = [(\alpha^6, 0), (\alpha^3, 1), (\alpha^5, 3), (\alpha^0, 4)]$,
$B = [(\alpha^1, 0), (\alpha^4, 2), (\alpha^3, 5), (\alpha^6, 6)]$.

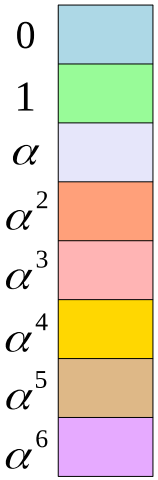


Figure 11: Symbols Color Code.

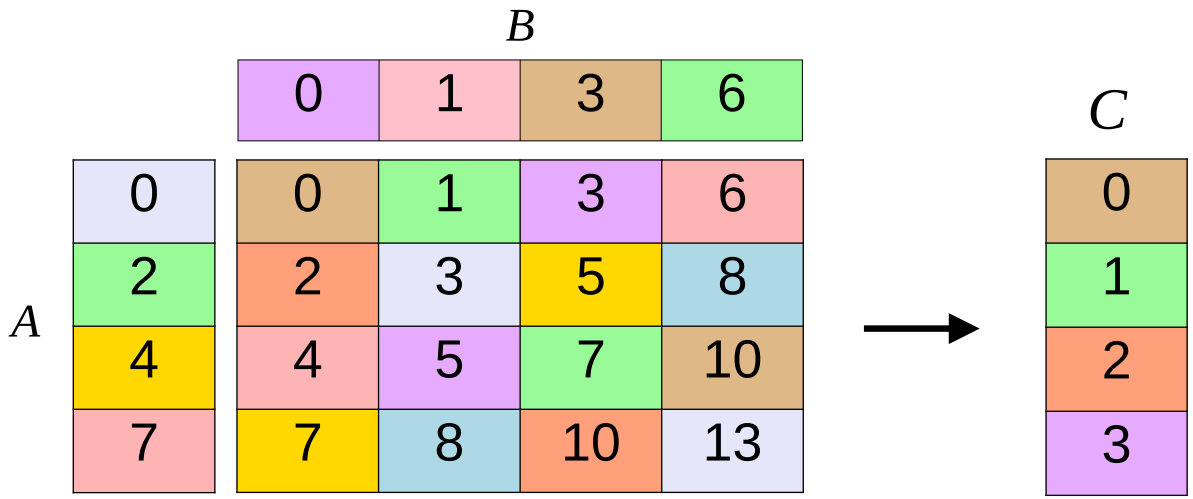
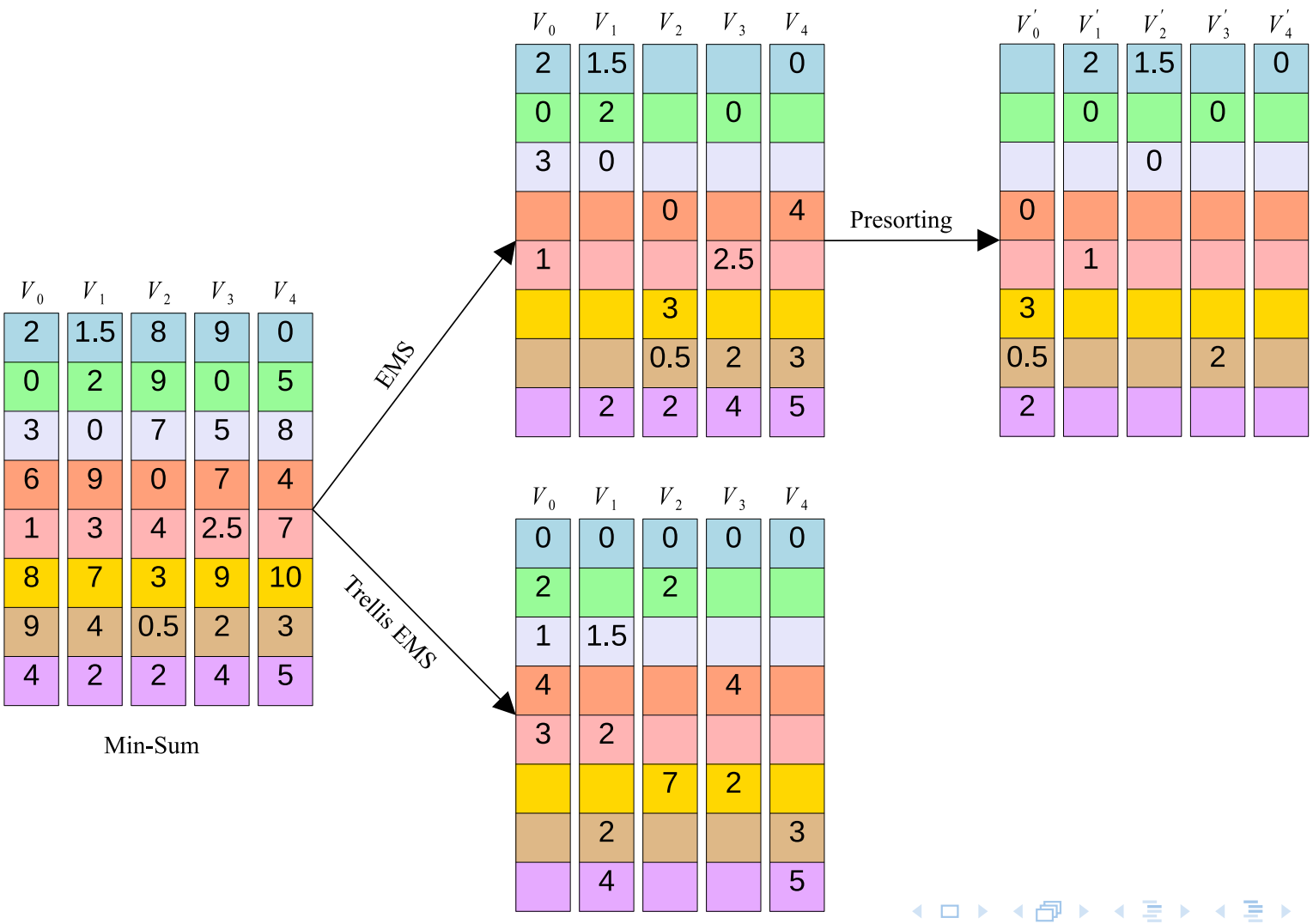


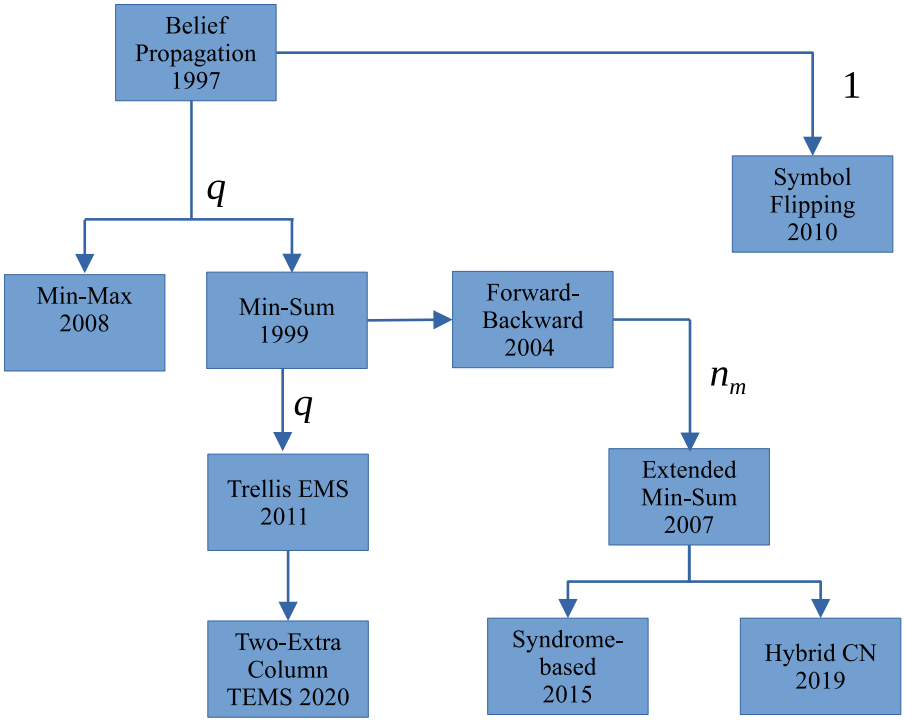
Figure 12: Processing of EMS-based ECN

Truncation Scheme for NB-LDPC Decoders



Evolution of NB-LDPC Decoding Algorithms.

- Belief Propagation[8].
- Symbol Flipping [10].
- Min-Max [11].
- Min-Sum [12].
- Extended Min-Sum [13].
- Syndrome-Based[14].
- Forward-Backward [15].
- L-Bubble [16].
- S-Bubble [17].
- Trellis Extended Min-Sum [18].
- Two-Extra Columns TEMS [19].

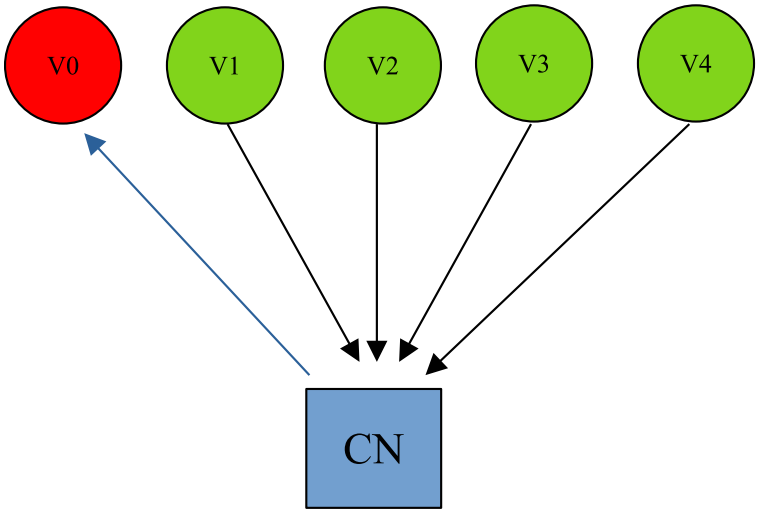


Is there still room for further reduction in complexity?

The Best, the Requested, and the Default Algorithm I

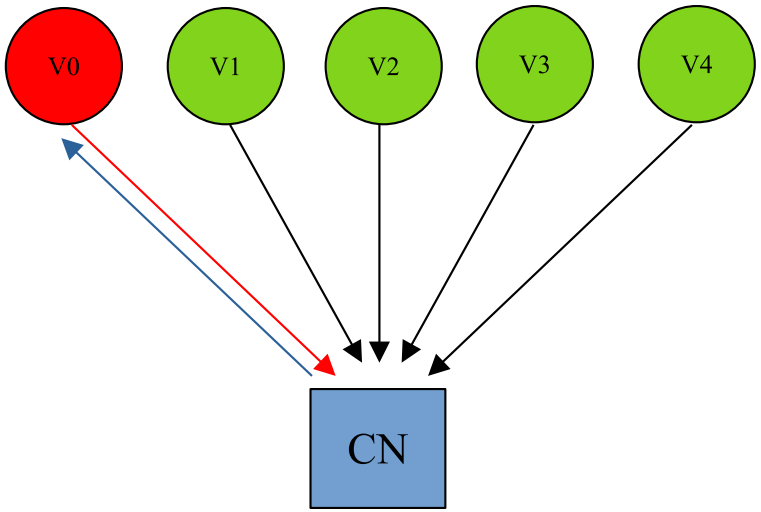
The intangible principle of iterative decoding..

A priori information are NEVER considered.

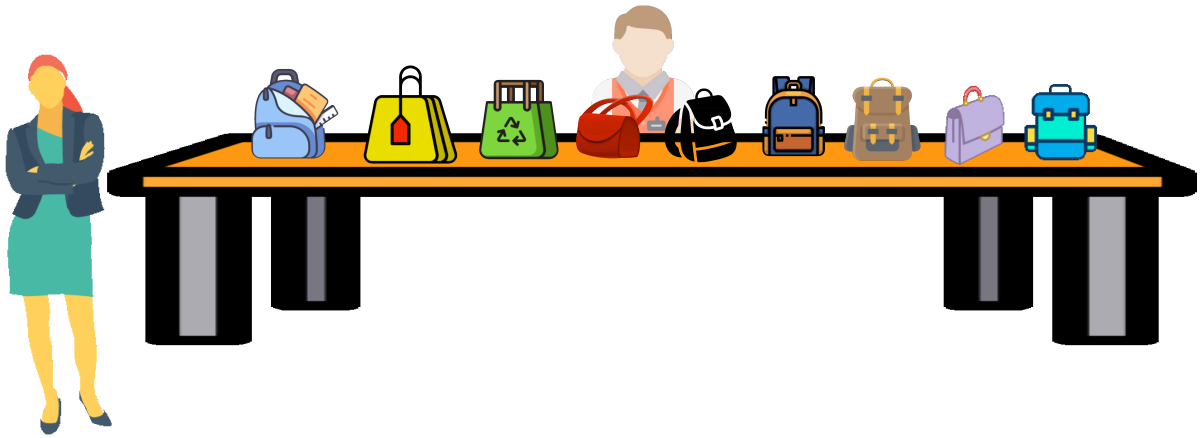


Is NO MORE intangible!

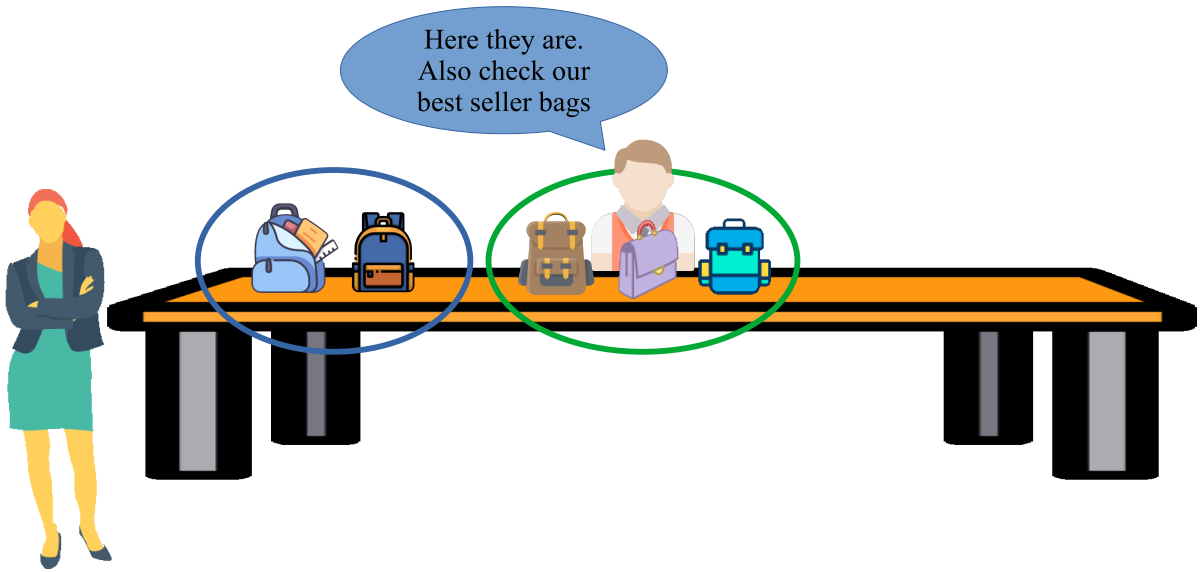
Considering A priori information (correctly) simplifies the decoding process!



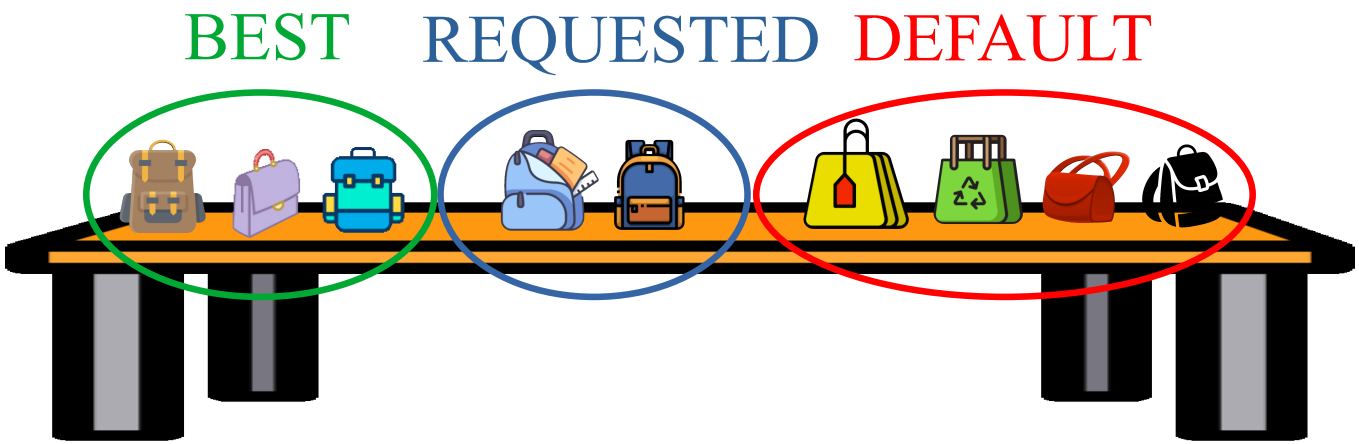
The Best, the Requested, and the Default in a Market I



The Best, the Requested, and the Default in a Market II



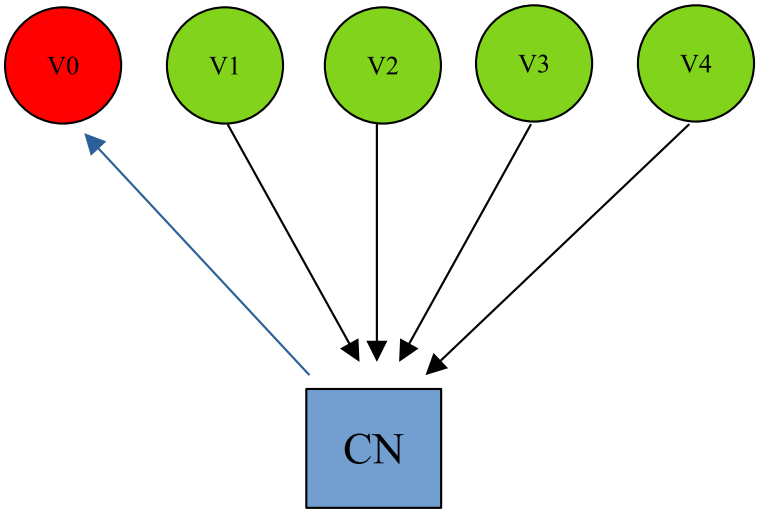
The Best, the Requested, and the Default in a Market III



The Best, the Requested, and the Default Algorithm I

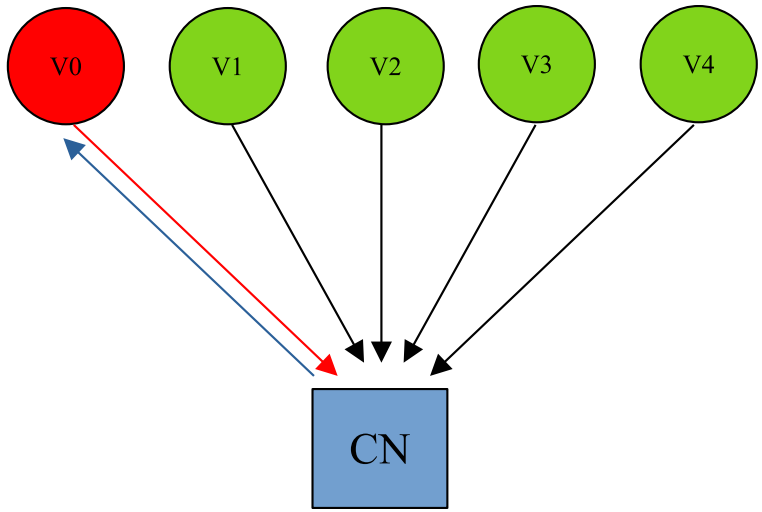
The intangible principle of iterative decoding..

A priori information are NEVER considered.



Is NO MORE intangible!

Considering A priori information (correctly) simplifies the decoding process!



The Best, the Requested, and the Default Algorithm II

- In BRD, VN requests the reliability of specific symbols from CN.
- Including these requested symbols maintains code convergence using fewer elements.
- Reduces communication load (bottleneck in parallel implementations) while maintaining similar decoding performance.

The Best, the Requested, and the Default Algorithm III

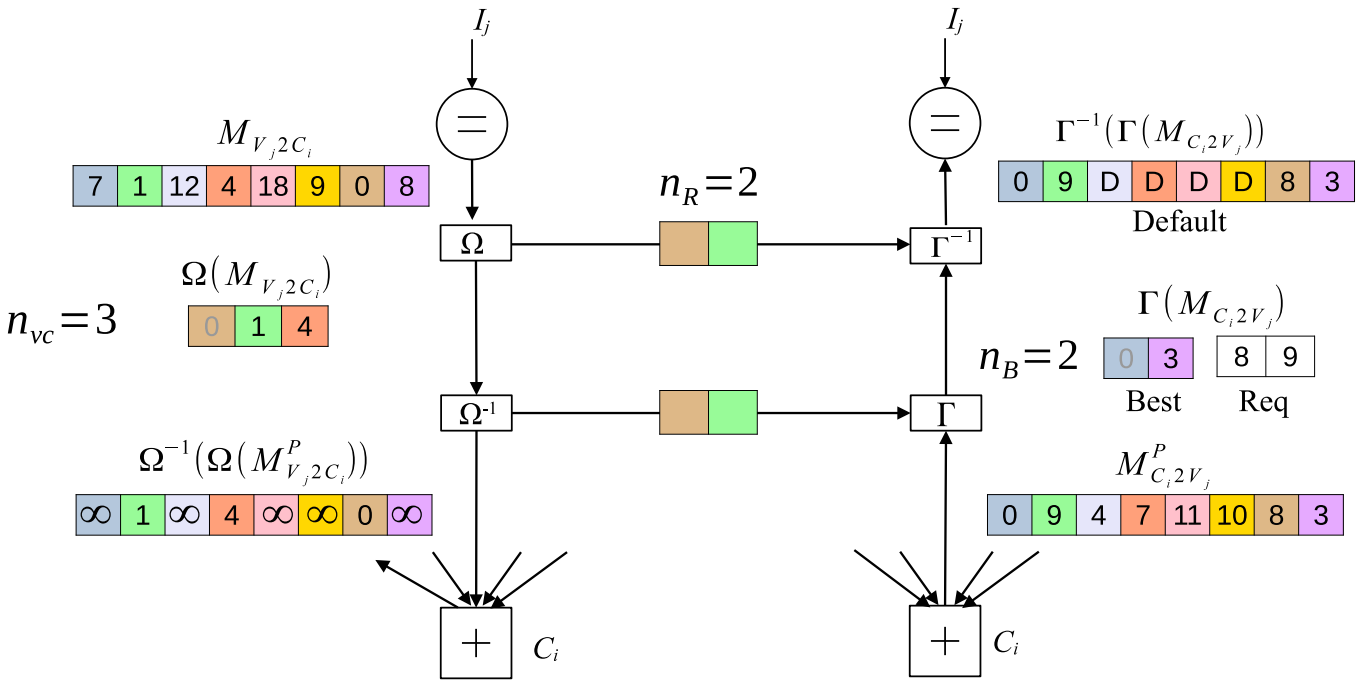


Figure 13: Toy Example on BRD over GF(8).

Statistical Analysis of BRD Algorithm

- $K = 120$.
- $N = 144$.
- GF(64).
- $E_b/N_0 = 3.5$ dB.
- $iter_{max} = 10$.
- $n_B = 4$.
- $n_R = 3$.

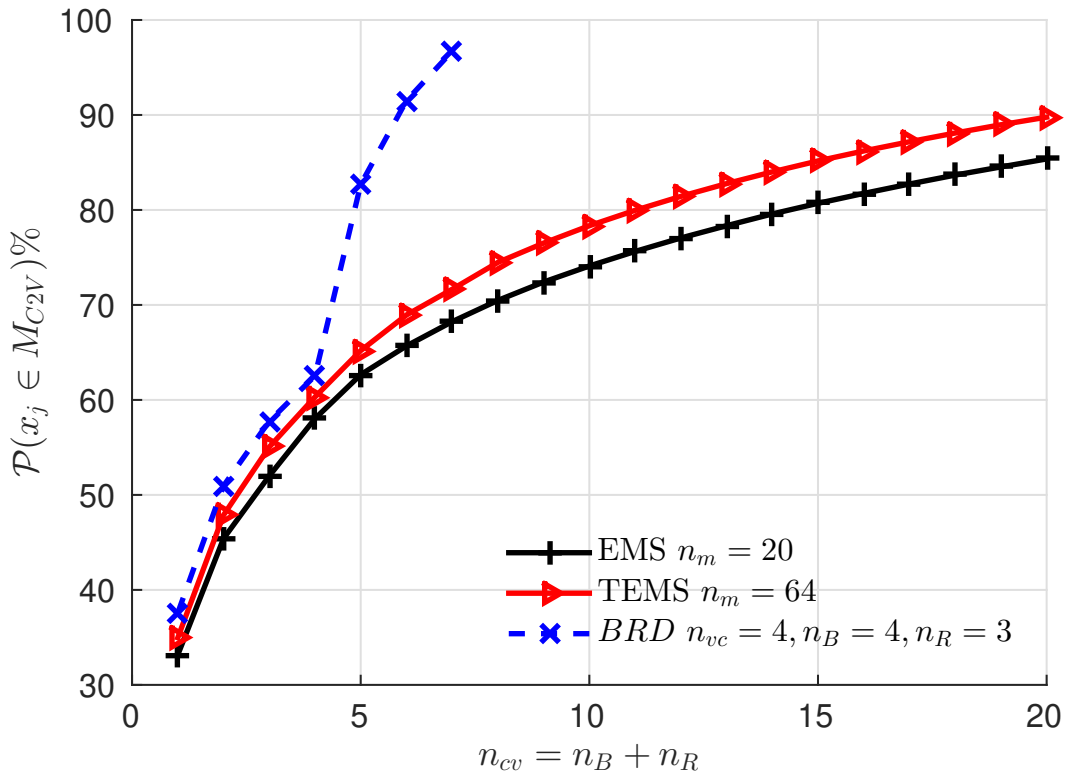


Figure 14: Probability that the encoded symbol x_j is in the message $\Gamma(M_{C2V_j})$.

Size of Messages

Table 1: Size of Exchanged Messages per Edge on GF(64)

Scheme	Code Rate	Input	Output	
		n_{vc}	n_B	n_R
TEMS	any	64	64	-
EMS	any	20	20	-
BRD	$r \geq 5/6$	4	4	3
	$r = 1/2$	8	6	5
	$r = 1/3$	13	7	8

Trellis BRD

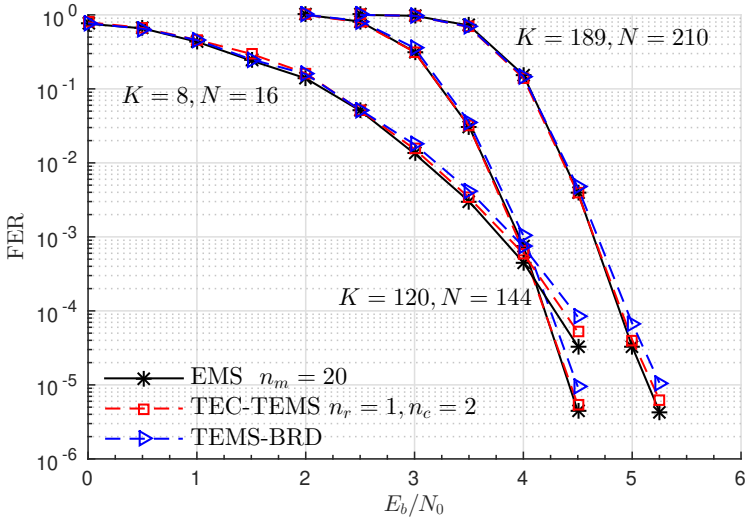


Figure 15: Trellis-BRD on GF(64) over BPSK.

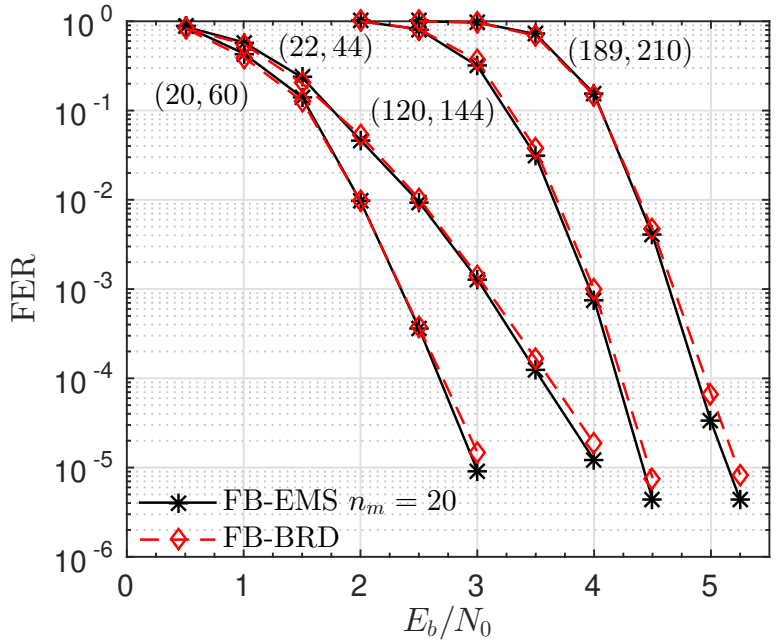


Figure 16: FB-BRD Decoder on GF(64) over BPSK.

Forward-Backward BRD Decoder I

Parallel CN implementation for a code rate $r = 5/6$ with $d_c = 12$ on Cyclone IV FPGA with frequency $F = 200$ MHz and throughput $T = 24$ Mbps.

Table 2: Synthesis Results for $d_c = 12$ on GF(64)

Scheme	Logic Elements	Registers
FB-EMS ($n_m = 16$)	109860	89940
FB-BRD ($n_{vc} = 4, n_B = 4, n_R = 3, n_{IN} = 15$)	94782	37308

15% reduction in computational load and 60% reduction in memory allocation.

NB-LDPC Conclusion

- The Best, the Requested, and the Default algorithm is proposed for NB-LDPC decoders.
- Reduces communication load by allowing exchange of a priori information.
- Implemented using different algorithms
  - Trellis EMS.
  - FB-EMS.
  - SYN-EMS.
- Also, used presorting to further reduce the internal processing of the EMS-based CN.

Non-Binary Polar Codes

Introduction to Non-Binary Polar Codes

- Latest error correction code proposed by E. Arikan in 2009[10].
- Encodes message of size K into a codeword of size N.
- Relies on channel polarization.
- Physical channel transformed into N virtual channels.
- Virtual channels are polarized into either noiseless or extremely noisy channels.

[10] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009. DOI: 10.1109/TIT.2009.2021379.

Structure of Polar Codes I

- Polar Code of code length N has $n = \log_2(N)$ (encoding/decoding) layers.
- Each layer consists of $N/2$ kernels.

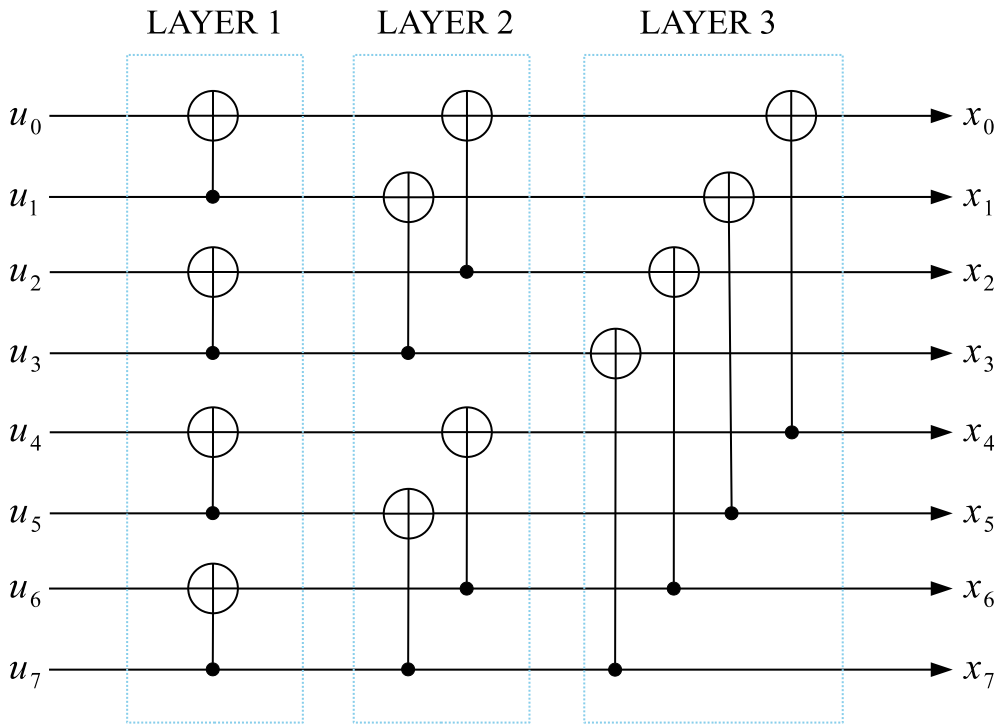


Figure 17: Polar Transformation (N-to-N) for $N = 8$.

Structure of Polar Codes II

- Kernel is basic processing unit in polar code.

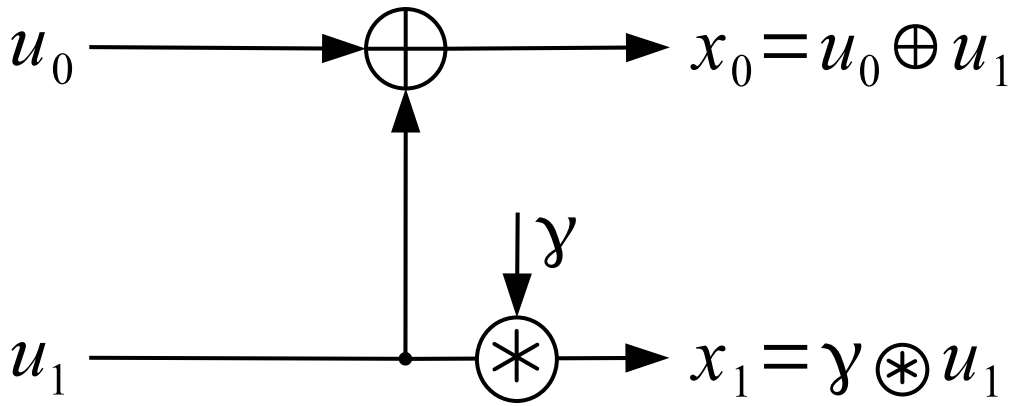


Figure 18: Encoding Kernel

Structure of Polar Codes III

Assume $K = 4$, $N = 8$. $\mathcal{A}_D = \{3, 5, 6, 7\}$ (using Genie-Aided decoding).

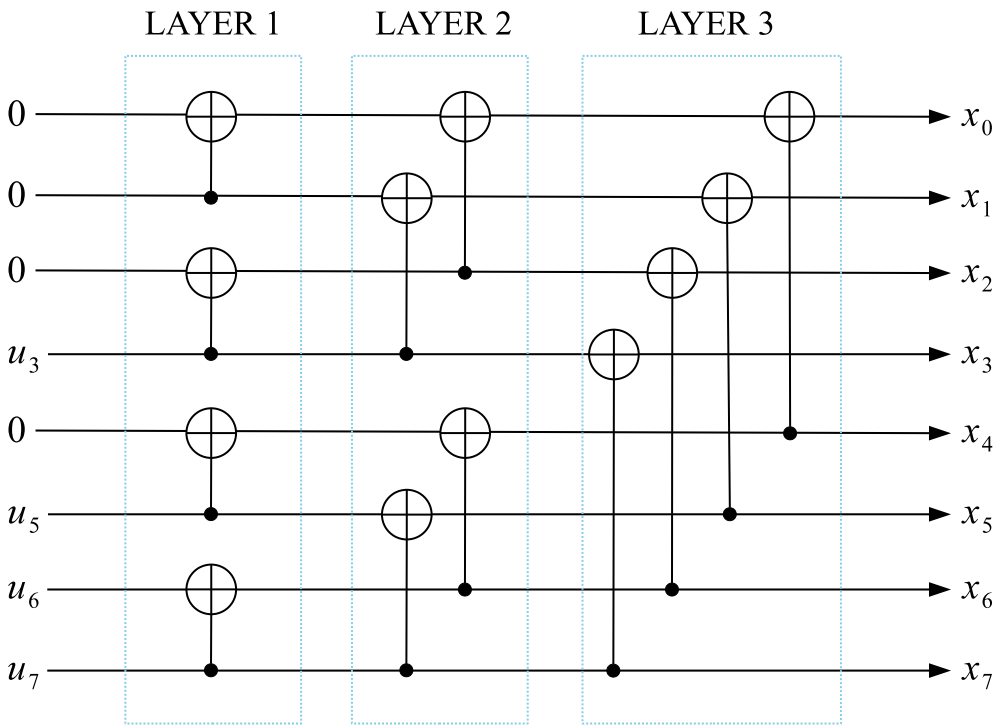


Figure 19: Polar Encoding

Structure of Polar Codes IV

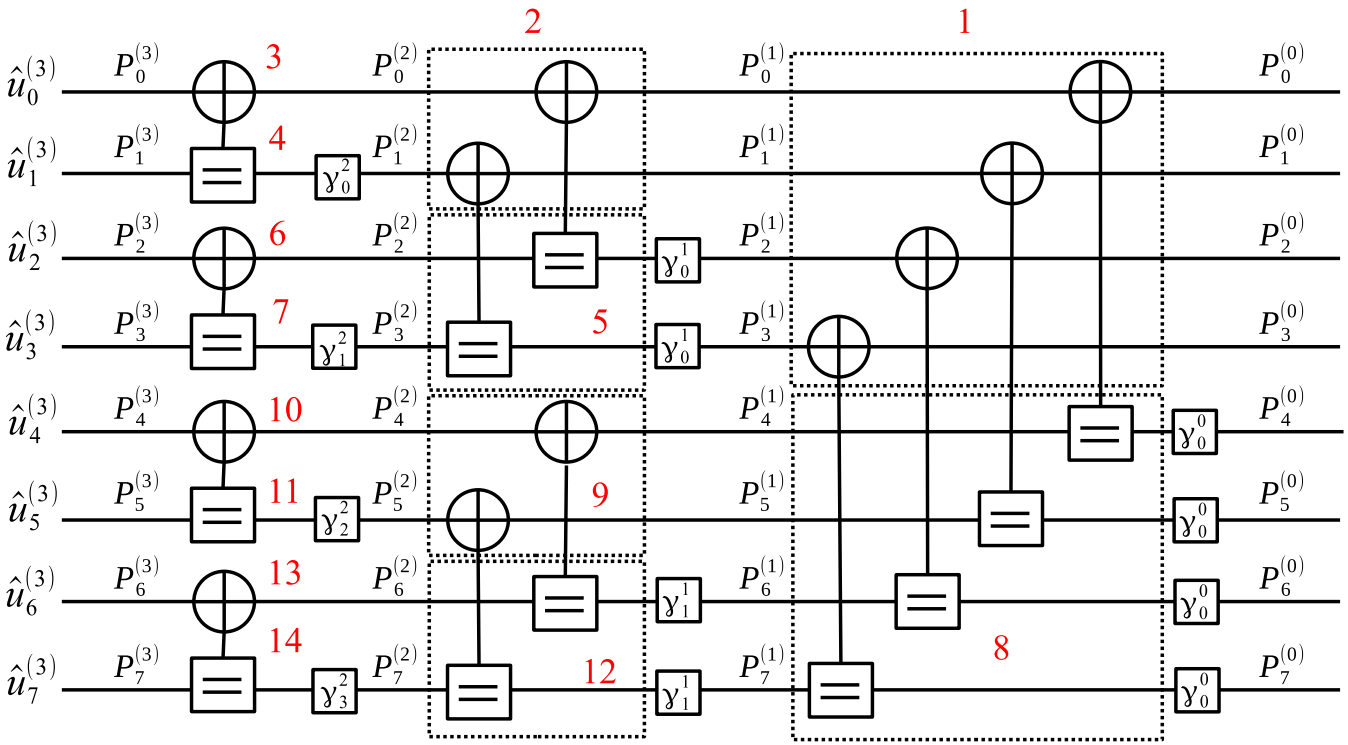


Figure 20: Factor Graph of SC Decoder for $N = 8$

Structure of Polar Codes V

Successive Cancellation (SC) Decoding

$$P_0^u(\alpha) = \sum_{\beta \in GF(q)} P_0^x(\alpha \oplus \beta) \cdot P_1^x(\gamma \circledast \beta) \; \forall \alpha \in GF(q). \tag{2}$$

$$\hat{u}_0 = \underset{\alpha \in GF(q)}{\operatorname{argmax}} \; P_0^u(\alpha), \tag{3}$$

$$P_1^u(\beta) = \mu \cdot P_0^x(\hat{u}_0 \oplus \beta) \cdot P_1^x(\gamma \circledast \beta) \; \forall \beta \in GF(q), \tag{4}$$

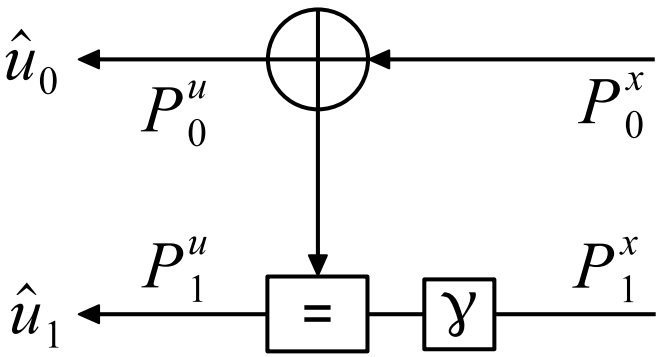


Figure 21: Decoding Process

Evolution of Non-binary Polar Decoding Algorithms

- Min-Sum[11]:
  - Eliminates complex functions such as logarithmic and exponential functions.
  - Converts all multiplication operations to additions.
- Simplified Min-Sum[12].
  - Truncation of one input only.
- Extended Min-Sum[13]:
  - Truncates the messages down to n_m.

[11] F. Cochachin, L. Luzzi, and F. Ghaffari, "Reduced Complexity of a Successive Cancellation Based Decoder for NB-Polar Codes," in *2021 11th International Symposium on Topics in Coding (ISTC)*, 2021.

[12] F. Cochachin and G. Fakhreddine, "A Lightweight Encoder and Decoder for Non-Binary Polar Codes," in *2023 22nd International Conference on Wireless Networks (ICWN)*, 2023.

[13] P. Chen, B. Bai, and X. Ma, "Non-Binary Polar Coding with Low Decoding Latency and Complexity," *Journal of Information and Intelligence*, 2022, ISSN: 2949-7159.

Asymmetrical Extended Min-Sum SC Decoder I

Check Node Processing:

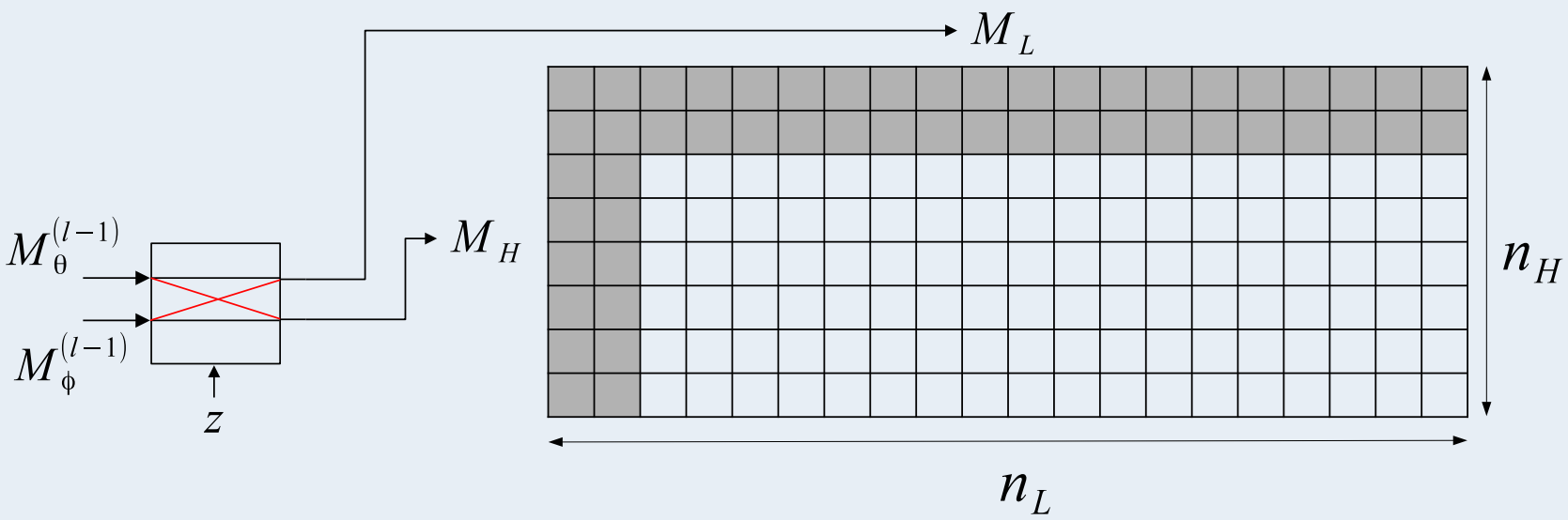


Figure 22: Schematic Structure of an AEMS CN.

Asymmetrical Extended Min-Sum SC Decoder II

Table 3: Arithmetic Operations Performed per CN

Algorithm	**GF Additions**	**Real Additions**
SC-MS	q^2	q^2
SC-EMS	$n_m\sqrt{n_m}$	$n_m\sqrt{n_m} - (2n_m - 1)$
SC-AEMS	$2(n_H + n_L) - 4$	$n_H + n_L - 3$

Compared to the EMS-based CN with $n_m = 20$, total computed candidates by an AEMS-based CN with $n_L = 20$ and $n_H = 8$ is reduced by 50%.

Asymmetrical Extended Min-Sum SC Decoder III

- CCSK+BI-AWGN.

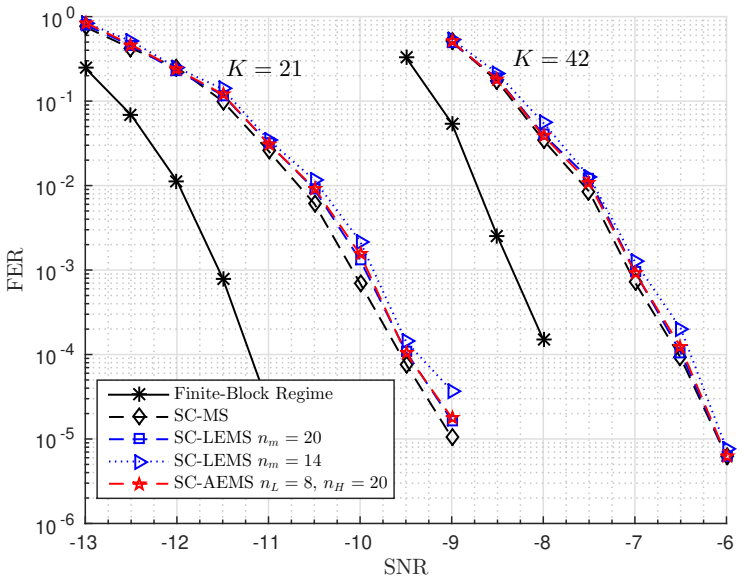


Figure 23: Simulation Results over $GF(64)$ for $N = 64$, $r \approx 1/3$ $(r_e \approx 1/32)$ and $r \approx 2/3$ $(r_e \approx 1/16)$ respectively.

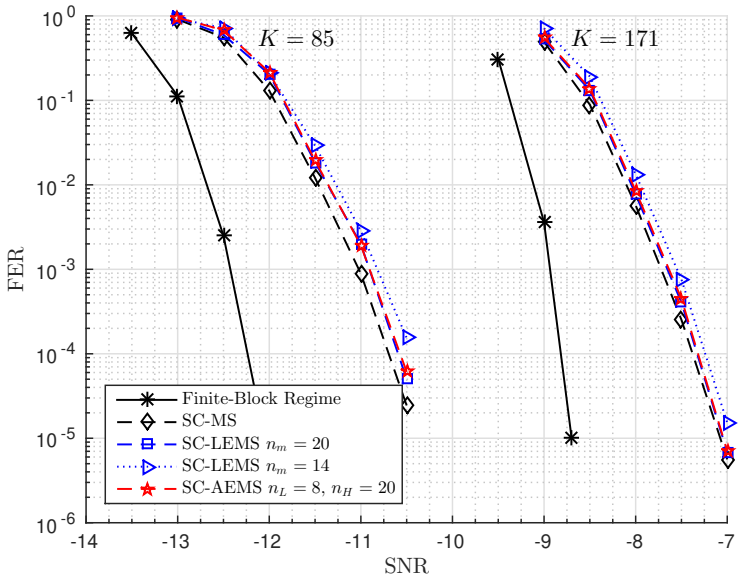


Figure 24: Simulation Results over $GF(64)$ for $N = 256$, $r \approx 1/3$ $(r_e \approx 1/32)$ and $r \approx 2/3$ $(r_e \approx 1/16)$ respectively.

Polarization-Aware SC Decoder

- Polarization-Aware SC (SC-PA) decoder is a tailored SC decoder that has different kernel processing and input sizes.
- Designed using statistical estimation of CNs on successfully decoded frames.

SC-PA: Node Clusters

- At each layer $l = 1, \cdots, n$, there are $s = \{0, \cdots, 2^{l-1}\}$ clusters.
- Each cluster s has set of kernels $S_s^{(l)}$ includes kernels from $t = s \times (2^{n-l})$ up to $t = (s+1) \times (2^{n-l}) - 1$.

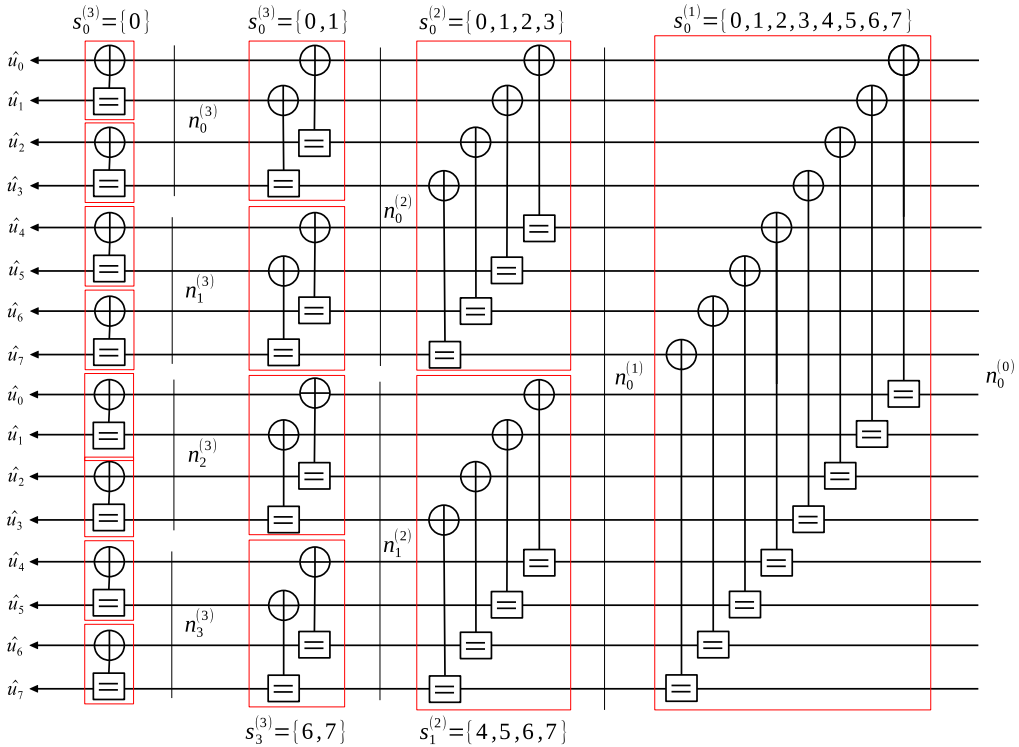


Figure 25: Nodes Clusters

SC-PA: Statistical Computation Using EMS CNs I

- Bubble pattern matrix $\mathcal{B}_t^{(l)}$ is defined as a matrix of size $n_m \times n_m$ which includes the occurrence of the element (bubble) of $T'_{\Sigma}(i,j)$.

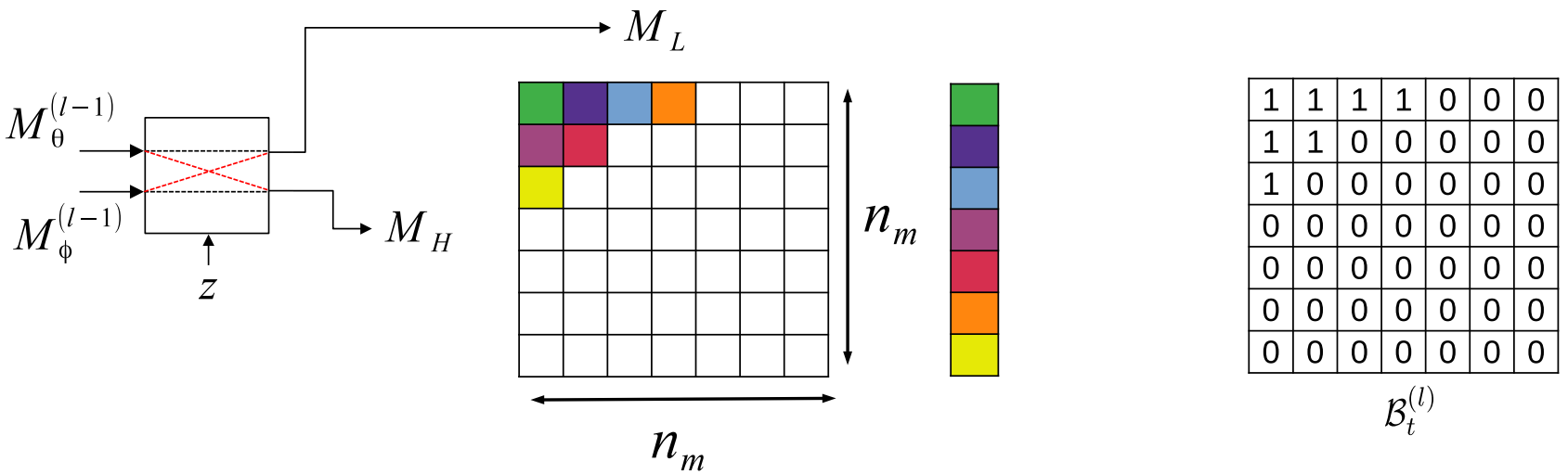


Figure 26: Computation of Bubble Indicator

SC-PA: Statistical Computation Using EMS CNs II

Contribution Rate Matrix: $$\mathcal{C}_s^{(l)} = \frac{1}{2^{n-l}} \sum_{t=s.2^{n-l}}^{(s+1).2^{n-l}-1} \mathcal{B}_t^{(l)}. \quad (5)$$

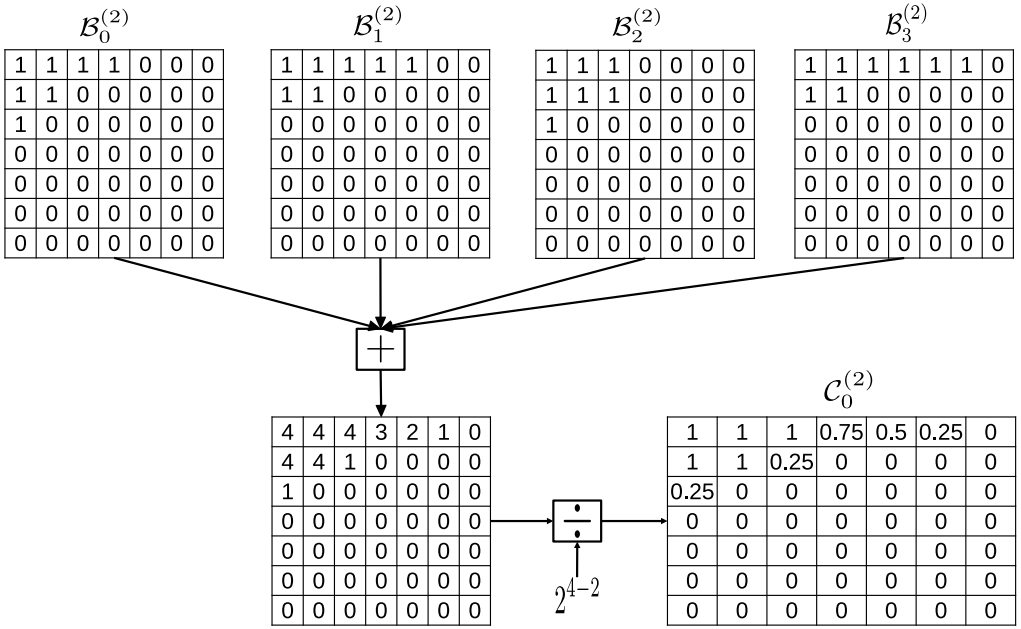


Figure 27: Computation of Contribution Rate Matrix

SC-PA: Statistical Computation Using EMS CNs III

Accumulate statistical estimation over N_r decoded frames.

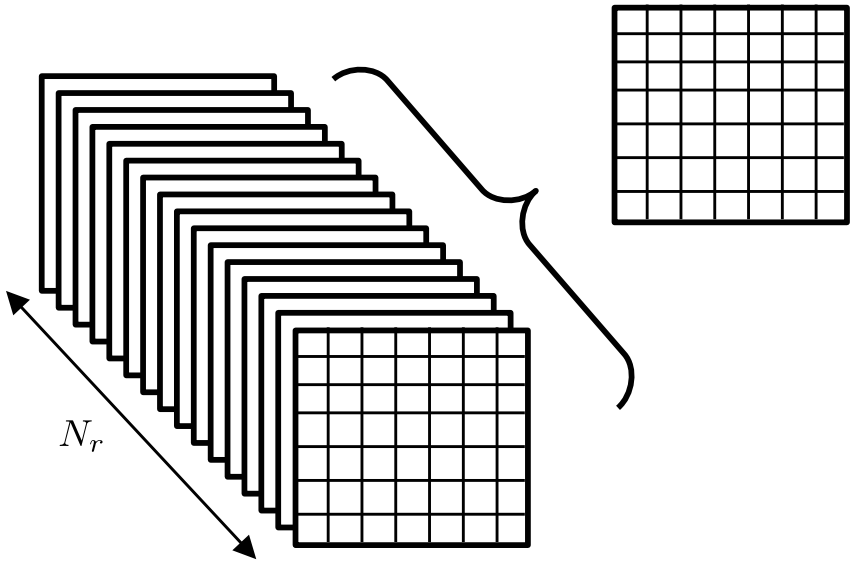


Figure 28: Accumulated Statistics of Contribution Rate Matrix

SC-PA: Pruning Process I

- Pruning process applied to T'_{Σ} of each cluster by defining threshold $\mathcal{P}_t$.
- Any bubble $T'_{\Sigma}(i,j)$ with contribution rate $\mathcal{C}_s^{(l)}(i,j) < \mathcal{P}_t$ is omitted from CN processing.
- Pruned matrix formed and denoted as $T'^{(l)}_{\Sigma_s}$ defined using indication matrix $\mathcal{R}_s^{(l)}$.

$$\mathcal{R}_s^{(l)} = \begin{cases} 1 & \text{If } \mathcal{C}_s^{(l)}(i,j) > \mathcal{P}_t \\ 0 & \text{Otherwise} \end{cases} . \tag{6}$$

$\mathcal{C}_0^{(2)}$

1	1	0.96	0.89	0.77	0.5	0.2
0.97	0.76	0.61	0.53	0.4	0.29	0.1
0.7	0.3	0.25	0.1	0.07	0.05	0.02
0.51	0.1	0.05	0	0	0	0
0.29	0.05	0.03	0	0	0	0
0.15	0.03	0.01	0	0	0	0
0.08	0.01	0	0	0	0	0

$\mathcal{P}_t = 0.3$ →

$\mathcal{R}_0^{(2)}$

1	1	1	1	1	1	0
1	1	1	1	1	0	0
1	0	0	0	0	0	0
1	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

Figure 29: Pruning Process to Generate Indicator Matrix

SC-PA: Pruning Process II

$$T'^{(l)}_{\Sigma_s}(i,j) = \begin{cases} M_H(i) \boxplus M_L(j) & \text{If } \mathcal{R}^{(l)}_s(i,j) = 1 \\ (0, +\infty) & \text{Otherwise} \end{cases} : 0 \leq i,j < n^{(l-1)}_{s'}, \tag{7}$$

where $n^{(l-1)}_{s'}$ is the size of the input messages (output size of the connected cluster in the previous layer), i.e., $s' = \lfloor s/2 \rfloor$.

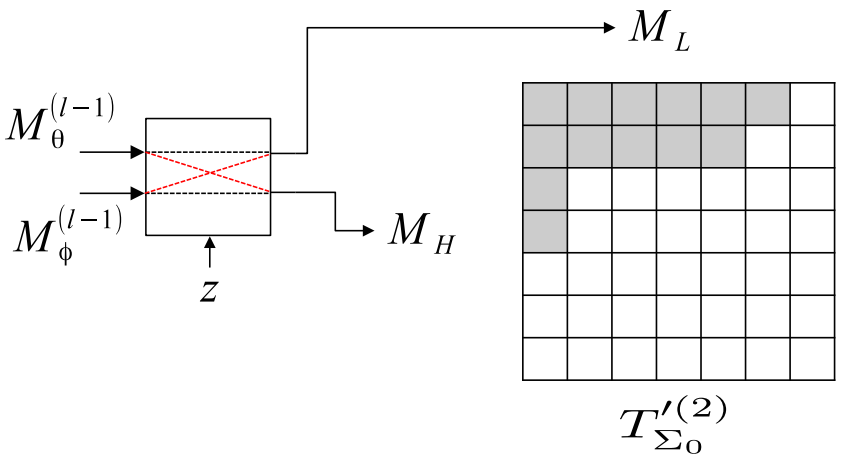


Figure 30: Pruned Matrix $T'^{(l)}_{\Sigma_s}$

SC-PA: Complexity and Simulation Results I

- $N = 256$.
- $K = 85$.
- GF(64).
- SNR$=-11.5$ dB.

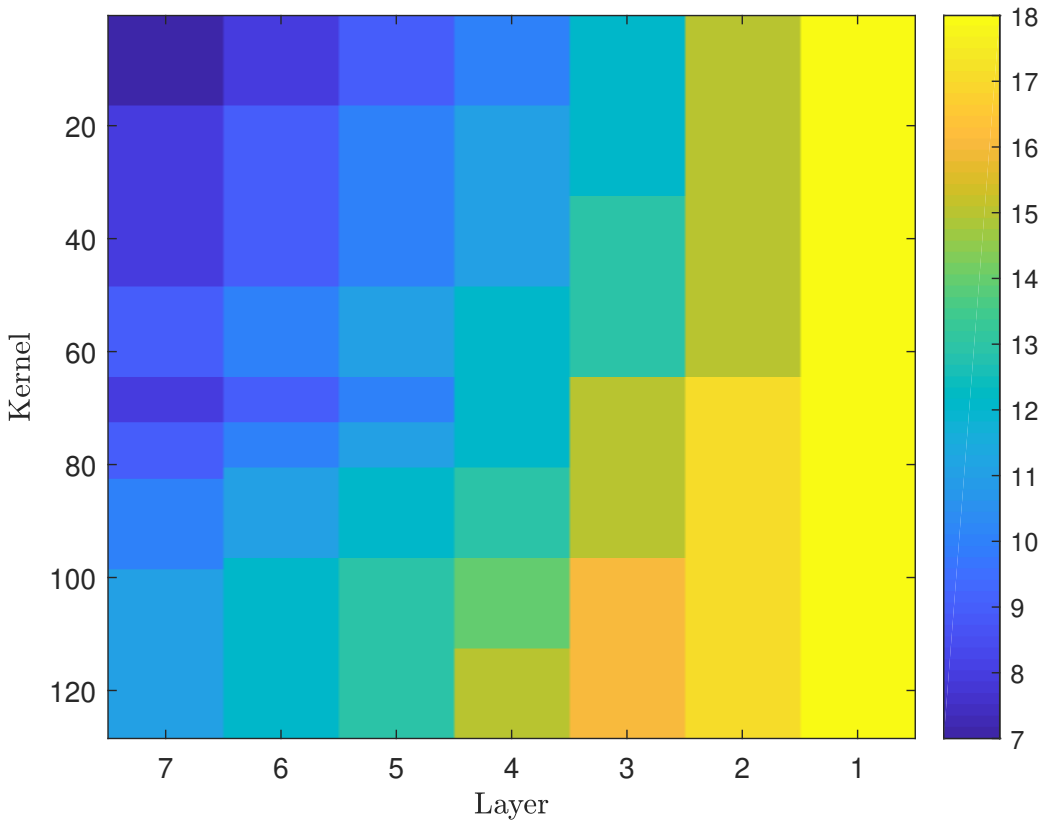


Figure 31: Size Map over Different Layers and Kernels.

SC-PA: Complexity and Simulation Results II

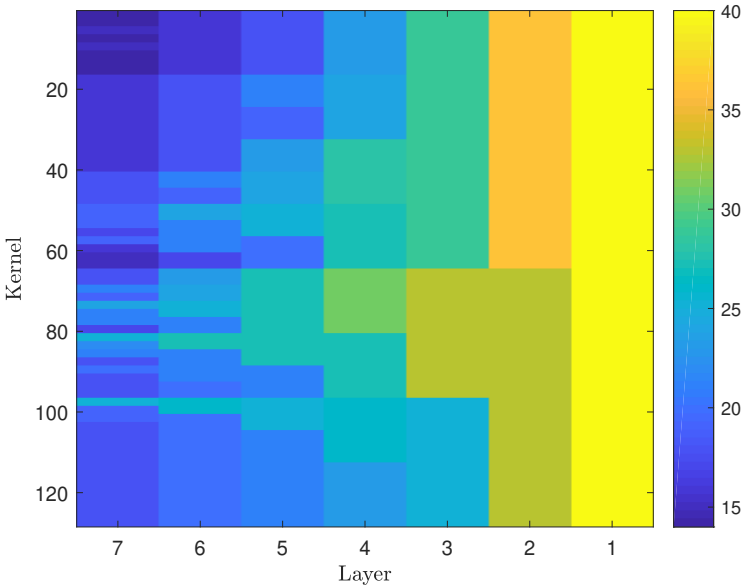


Figure 32: GF Additions per Kernel CN.

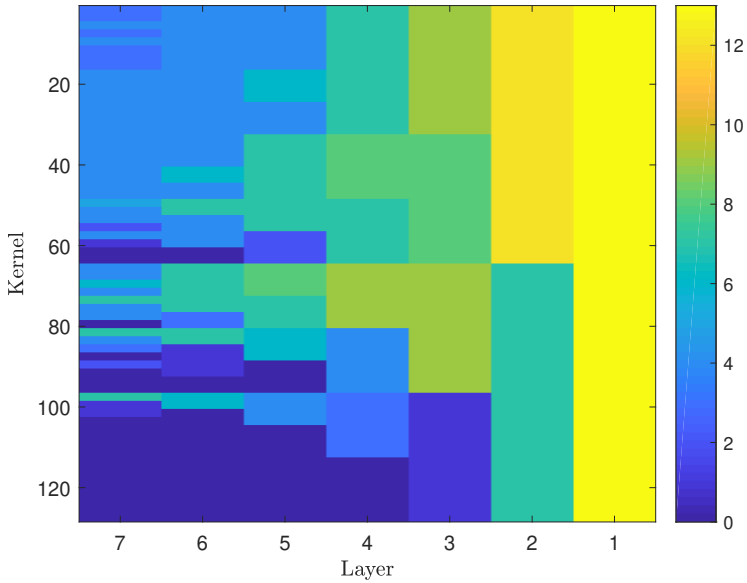


Figure 33: LLR Additions per Kernel CN.

SC-PA: Complexity and Simulation Results III

Table 4: Design Parameters for SC-PA Decoder and Arithmetic Operations over Different Codes.

K	μ	SC-PA		SC-AEMS		SC-EMS	
		T_{GF}	T_{LLR}	T_{GF}	T_{LLR}	T_{GF}	T_{LLR}
$N = 64, \mathcal{P}_t = 0.12, n_0^{(0)} = 18$				$n_L = 20, n_H = 8$		$n_m = 18$	
11	-13.5 dB	3776	916	8320	4000	12160	6560
21	-10.5 dB	4082	788				
42	-7.5 dB	4370	424				
$N = 256, \mathcal{P}_t = 0.08, n_0^{(0)} = 18$				$n_L = 20, n_H = 8$		$n_m = 18$	
42	-14 dB	22362	6048	46592	22400	68096	36736
85	-11.5 dB	24294	5744				
171	-8 dB	24742	3180				
$N = 1024, \mathcal{P}_t = 0.09, n_0^{(0)} = 25$				$n_L = 20, n_H = 8$		$n_m = 22$	
171	-15 dB	151986	45756	239616	115200	474264	276480
341	-12 dB	180396	45420				
683	-8.5 dB	222488	33314				

50% saving in GF additions and 90% in LLR additions compared to SC-EMS.

SC-PA: Complexity and Simulation Results IV

- B1-SCL32
  - Binary SCL with $L = 32$.
  - $K_b = Kp$.
  - $N_b = Nq$.
  - $r = \dfrac{K_b}{N_b}$.

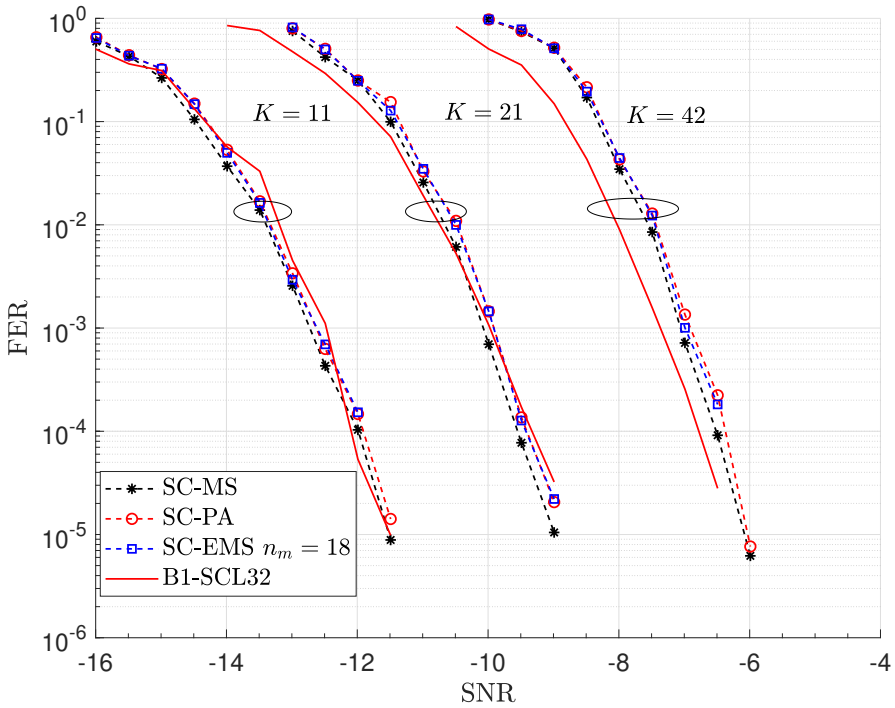


Figure 34: FER Performance over CCSK Modulation for $N = 64$ on GF(q).

SC-PA: Complexity and Simulation Results V

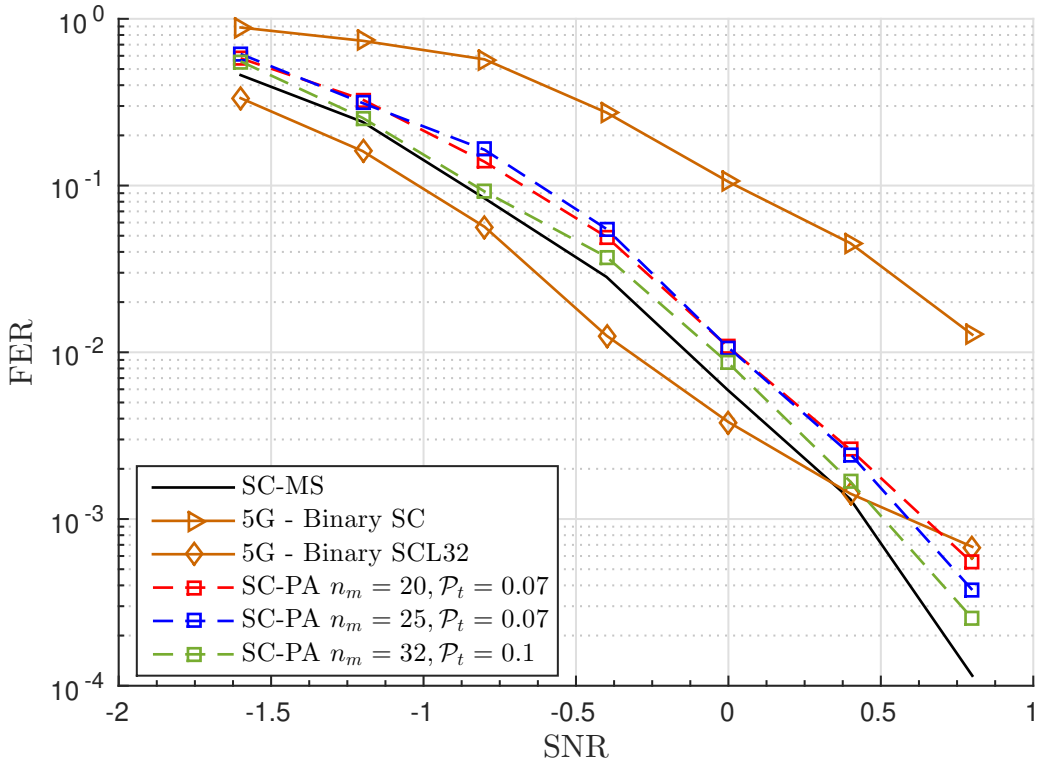
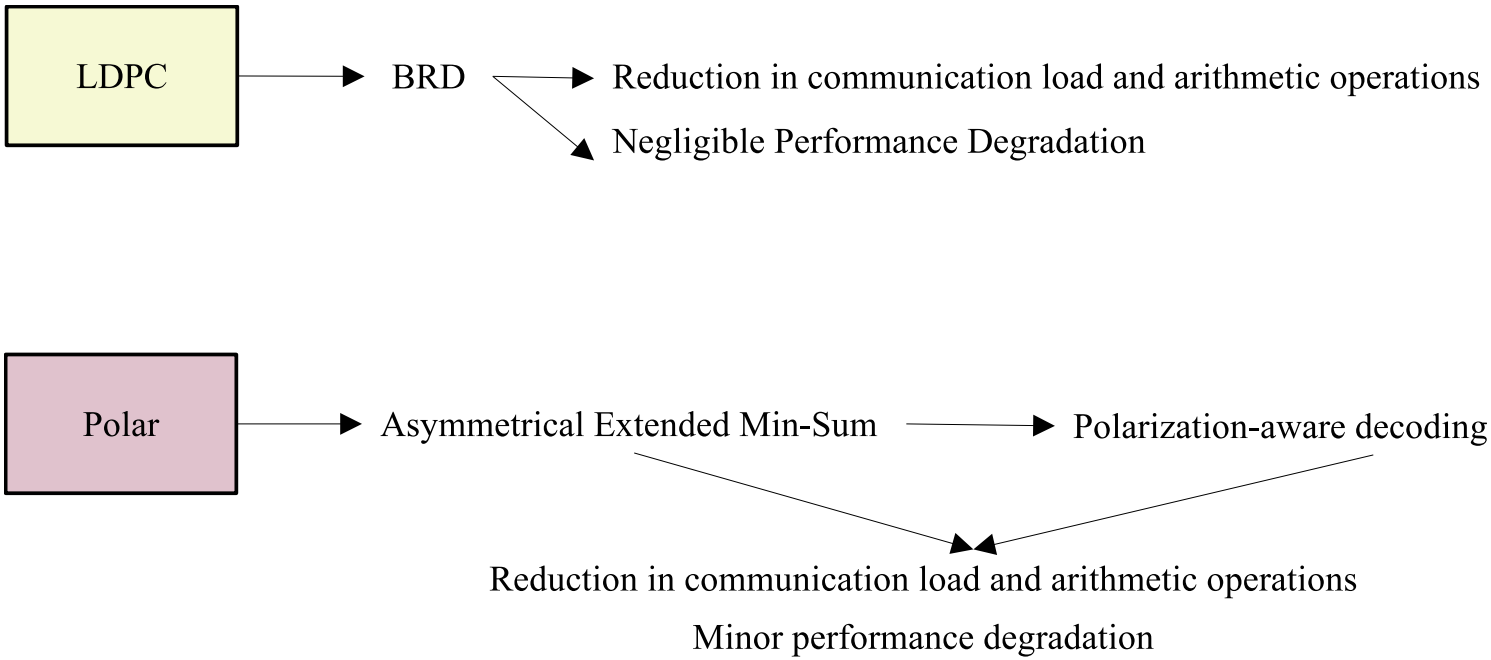


Figure 35: SC-PA over BPSK for $N = 128$, $K = 42$ on GF(64).

Conclusion

Non-binary codes outperform binary codes but suffer from higher complexity.



Thesis objective met :)

Perspectives and Future Work

- Overall complexity assessment:
  - Sorting.
  - VN Processing.
  - Routing.
  - Memory allocation.
- Hardware Implementation of proposed algorithms.
- Comprehensive complexity-performance study of non-binary polar and binary polar decoders over non-binary modulation.
- Extend study area to include SC List Decoding for NB Polar codes.
- Non-binary turbo codes.. a vague journey?

Thank You !

List of Publications

- J. Jabour, C. Marchand, and E. Boutillon, "The Best, The Requested, and The Default Non-Binary LDPC Decoding Algorithm," in *2021 11th International Symposium on Topics in Coding (ISTC)*, 2021, pp. 1–5. DOI: 10.1109/ISTC49272.2021.9594148
- J. Jabour, C. Marchand, and E. Boutillon, "The Best, the Requested, and the Default Elementary Check Node for EMS NB-LDPC Decoder," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, 2023, pp. 1–6. DOI: 10.1109/WCNC55385.2023.10118720
- J. Jabour, A. C. Al-Ghouwayel, and E. Boutillon, "Asymmetrical Extended Min-Sum for Successive Cancellation Decoding of Non-Binary Polar Codes," in *2023 12th International Symposium on Topics in Coding (ISTC)*, 2023, pp. 1–5. DOI: 10.1109/ISTC57237.2023.10273502
- J. Jabour, A. C. Al-Ghouwayel, and E. Boutillon, "Polarization-Aware Decoding for Non-binary Polar Decoders," *IEEE Communication Letters*, 2023. DOI: Submitted
- E. Boutillon, J. Jabour, and M. Cédric, "A method for decoding a codeword encoded using a non-binary code, corresponding device, and computer program," WO2023025960A1, 2023. [Online]. Available: https://patents.google.com/patent/WO2023025960A1

Complexity Comparison of Non-Binary LDPC Decoder

- $d_v = 2$:
  - $\frac{2N}{d_c}$ CN Processing.
  - Total of $6N - \frac{4N}{d_c}$ ECNs per iteration.
  - For $iter_{max} = 10$: $60N - \frac{20N}{d_c}$.

Complexity Comparison of Non-Binary Polar Decoder

- Each CN is an ECN.
  - $N/2$ CNs per layer.
  - $n-1$ layers.
  - Total of $(n-1).\frac{N}{2}$ ECNs.

Complexity Comparison of Non-Binary Decoder

- $N = 128$, $K = 64$.
  - LDPC: $6400N$ ECNs.
  - Polar: 384 ECNs.

Forward-Backward Approach for EMS CN I

1. Generating $T_\Sigma = A + B \rightarrow$ GF and LLR additions.
2. Extract n_{op} elements out of n_m^2.
3. Eliminate Redundancy to generate n_m unique candidates.

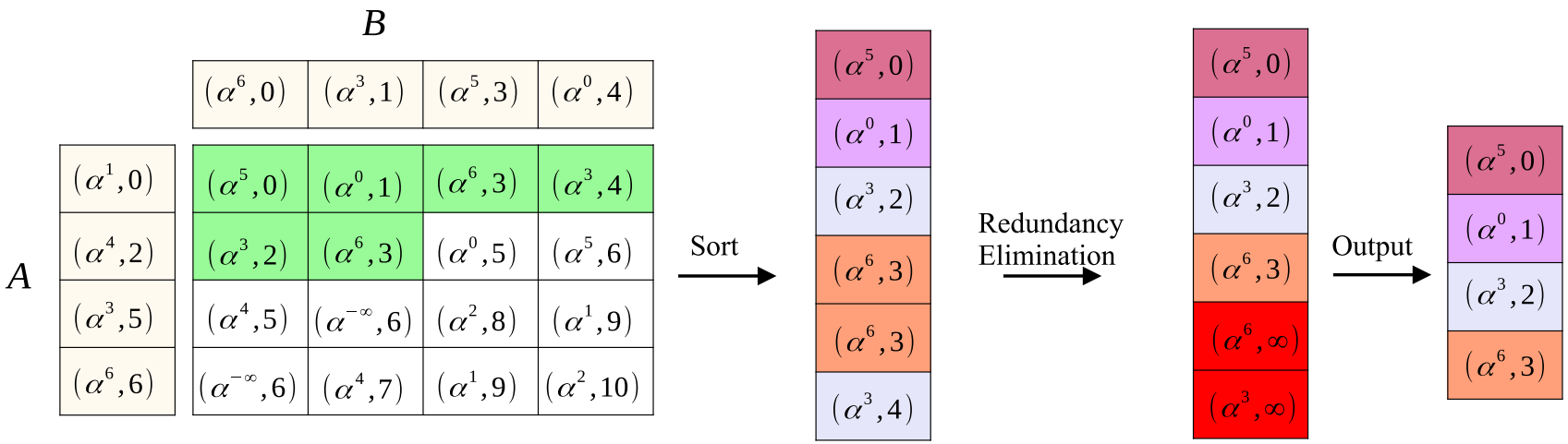


Figure 36: ECN Internal Processes

Still inefficient.. computing n_m^2 to generate n_m! Different solutions proposed.

Forward-Backward Approach for EMS CN II

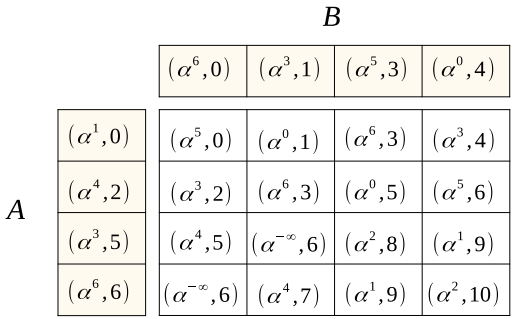


Figure 37: Bubble Check[14]

GF Add: $n_m\sqrt{n_m}$.
LLR Add: $n_m\sqrt{n_m} - 2n_m + 1$.

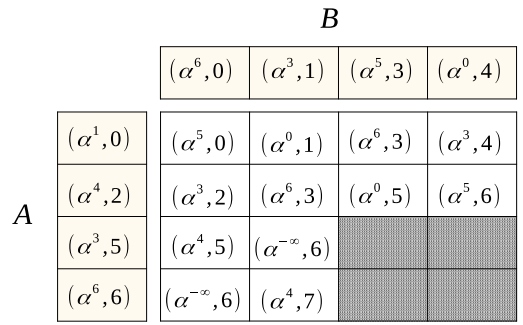


Figure 38: L-Bubble Check[15]

GF Add: $4n_m - 4$.
LLR Add: $2n_m - 3$.

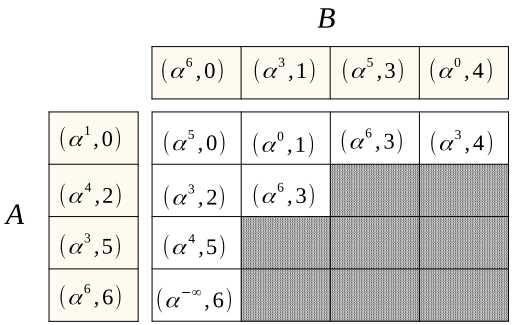


Figure 39: S-Bubble Check[16]

GF Add: $3n_m - 4$.
LLR Add: $n_m - 3$.

[20] E. Boutillon and L. Conde-Canencia, "Bubble check: a simplified algorithm for elementary check node processing in Extended Min-Sum non-binary LDPC decoders," *IEE Electronics Letters*, vol. 46, no. 9, pp. 633–631, 2010

[21] E. Boutillon and L. Conde-Canencia, "Simplified check node processing in nonbinary LDPC decoders," in *2010 6th International Symposium on Turbo Codes Iterative Information Processing*, 2010, pp. 201–205. DOI: 10.1109/ISTC.2010.5613839

[22] O. Abassi, L. Conde-Canencia, A. Al Ghouwayel, *et al.*, "A Novel Architecture for Elementary-Check-Node Processing in Nonbinary LDPC Decoders," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 2, pp. 136–140, 2017. DOI:

Syndrome-based EMS CN

- Parallel approach relies on deviation paths for generating syndromes.
- d_k elements are considered for syndromes computation (from each check node) with k deviations from the zeroth element of each input vector.

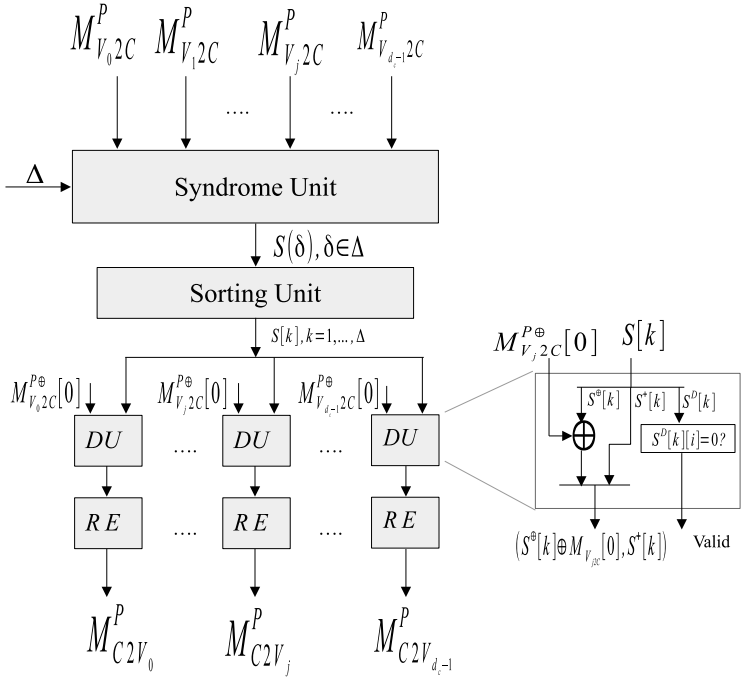


Figure 40: Syndrome-based Check Node

Trellis Extended Min-Sum

- Reduces complexity over high rate, i.e., d_c values.
- Delta domain transformation with no truncation or sorting.
- n_r (out of d_c LLR values are selected for each symbol).
- Configurations are built with n_c deviations only.

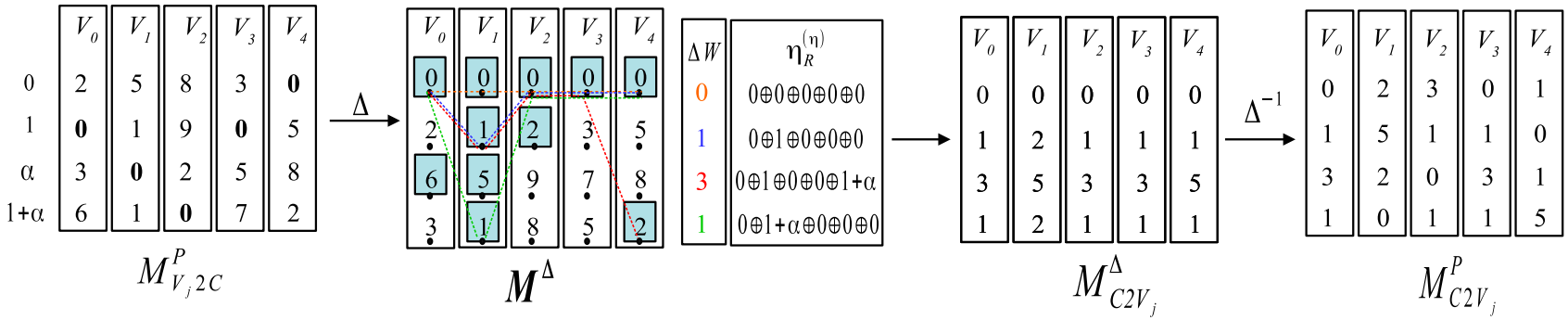


Figure 41: Example of Trellis EMS on GF(8) and $d_c = 5$.

Presorting Algorithm

Do we need to consider the same input size for all V2C messages?

- No, we do not!
- Polarize the inputs and omit useless input elements.
- Used with Syndrome-based CN[17] and Forward-Backward CN[18].

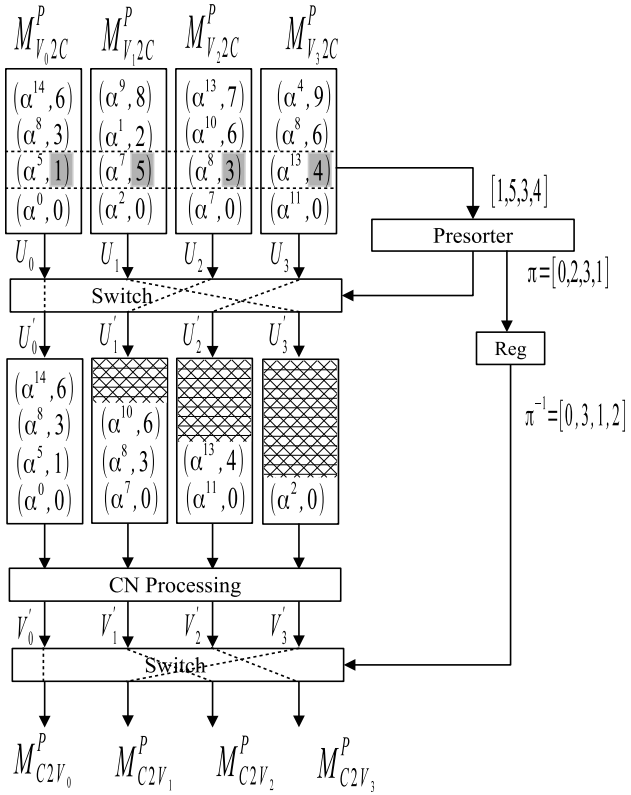


Figure 42: Presorting Algorithm

[20] C. Marchand and E. Boutillon, "NB-LDPC check node with pre-sorted input," in *2016 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*, 2016, pp. 196–200. DOI: 10.1109/ISTC.2016.7593104

Example on BRD over GF(8) I

- Compresses $M_{V_j 2C_i}$ from q down to n_{vc}.
- Send request message $M_j^{R\oplus}$ of n_R GF symbols (most reliable of $M_{V_j 2C_i}$) to Γ^{-1} block.

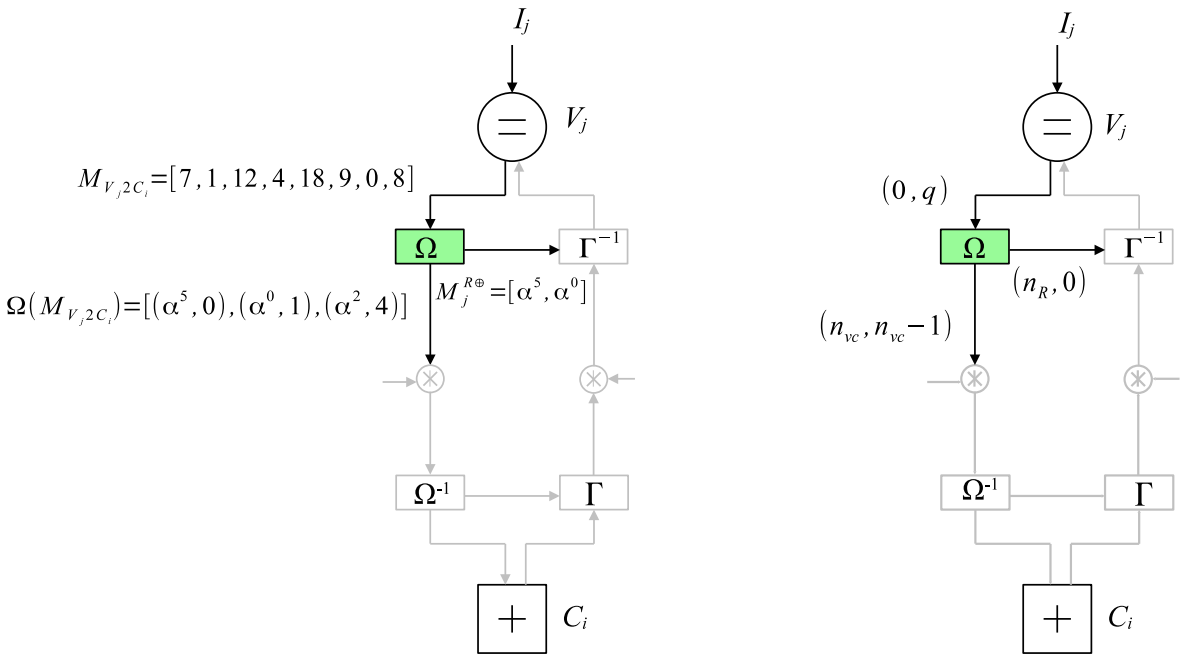


Figure 43: Ω Compression Block with $n_{vc}=3$ on GF(8).

Example on BRD over GF(8) II

- Decompresses $\Gamma(M^P_{V_j 2C_i})$ from n_{vc} to q.
- Send request message $M_j^{R\oplus}$ of n_R GF symbols to Γ^{-1} block.

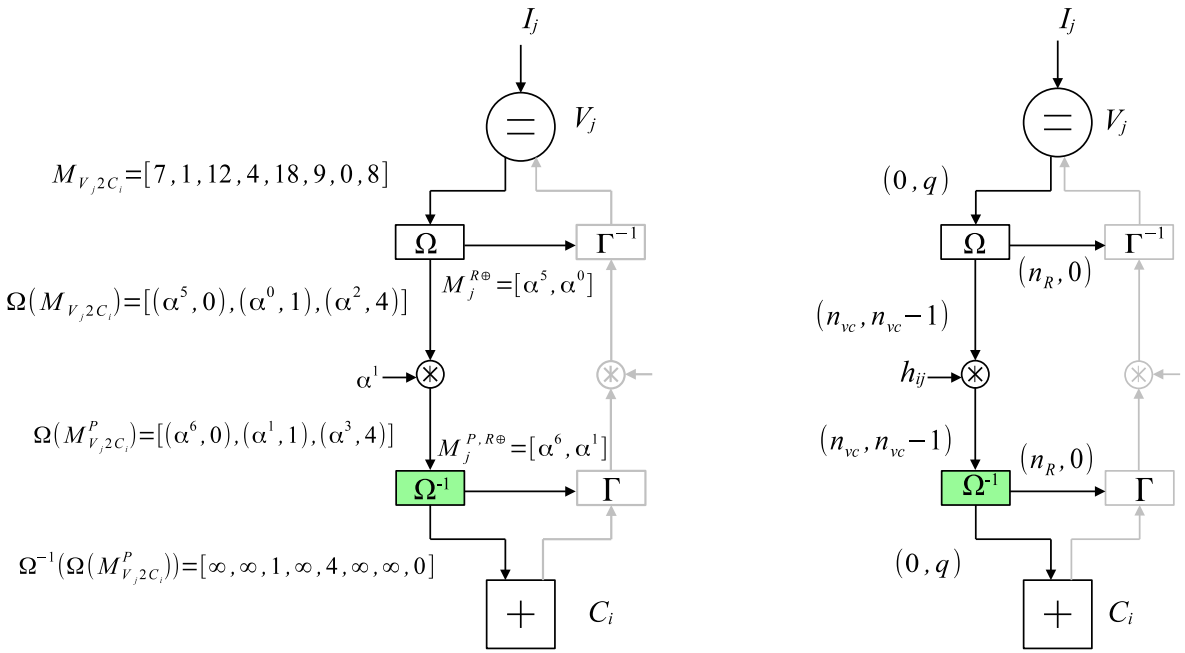


Figure 44: Ω Decompression Block with $n_R = 2$.

Example on BRD over GF(8) III

- n_B most reliable candidates are selected to generate subset $M^{P,B}_{C2V_j}$.
- LLR of the n_R requested symbols of $M^{P,R\oplus}$ are extracted from $M^{P}_{C2V_j}$.

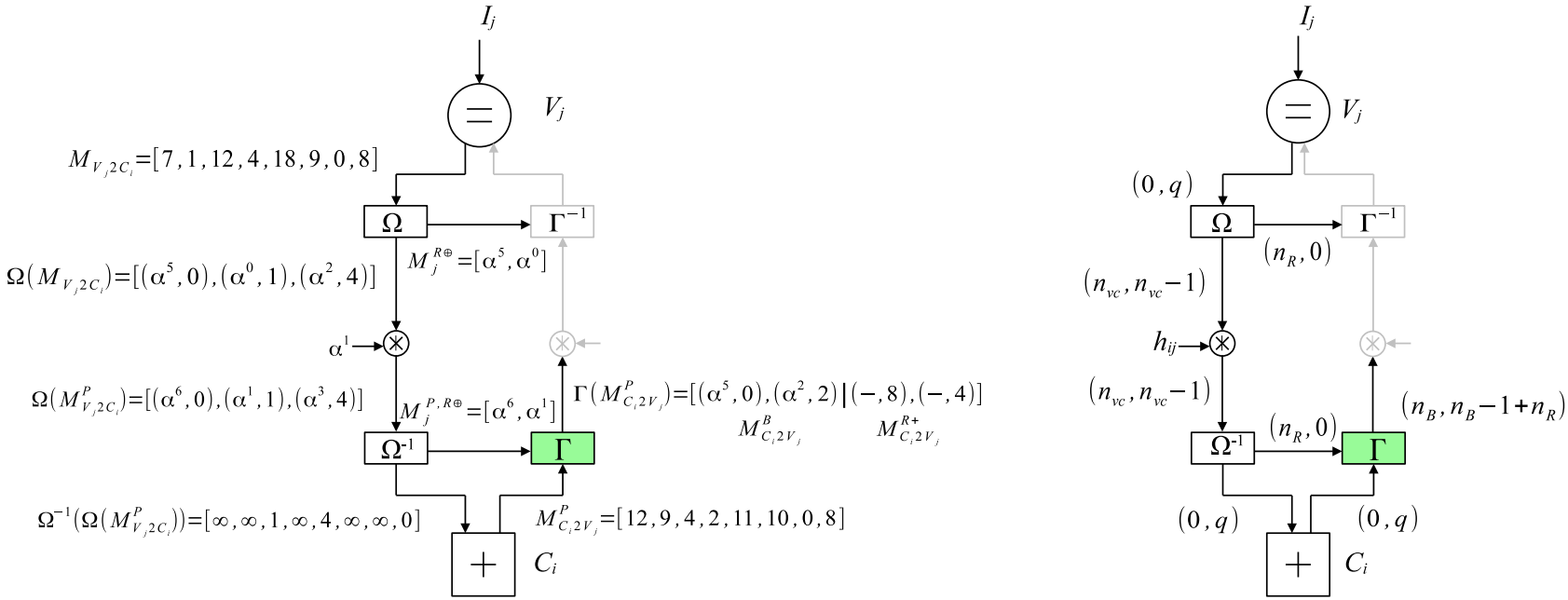


Figure 45: Γ Compression Block with $n_B = 2$ and $n_R = 2$.

Example on BRD over GF(8) IV

$$\Gamma^{-1}(\Gamma(M^{+}_{C2V_j}))[a] = \begin{cases} M^{B+}_{C2V_j}[a], & a \in M^{B\oplus}_{C2V_j} \\ \min\left(M^{R+}_{C2V_j}[a], S_R\right), & a \in M^{R\oplus}_{j} \\ S_D, & Otherwise \end{cases} \tag{8}$$

$$S = \gamma_B \cdot \max\{M^{B+}_{C2V_j}\} + \gamma_R \cdot \max\{M^{R+}_{C2V_j}\} \tag{9}$$

Requested Saturation: $S_R = S + O_R$
Default Saturation: $S_D = S + O_D$

Example on BRD over GF(8) V

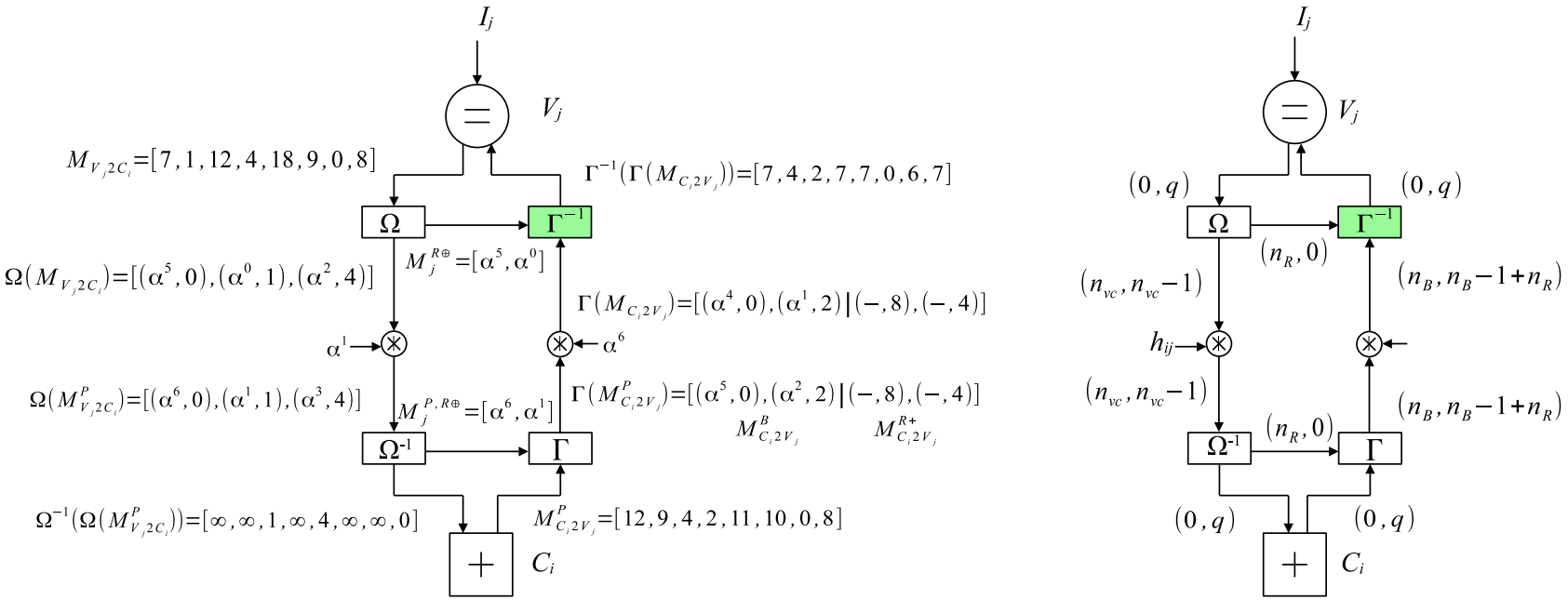


Figure 46: Γ Decompression Block with $n_B = 2$ and $n_R = 2$.

$$\gamma_R = 1, \gamma_B = 1,\ O_D = 1,\ O_R = 0 \rightarrow S_R = 6,\ S_D = 7.$$

Syndrome-based BRD Decoder

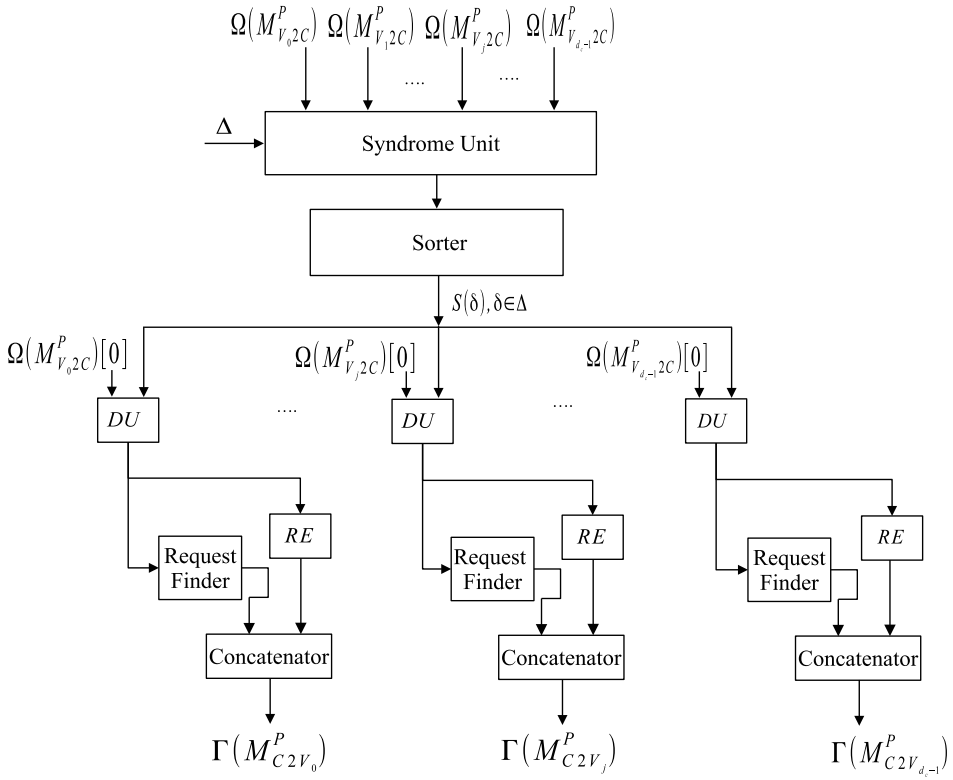


Figure 47: Syndrome-Based BRD

Presorted SYN-BRD Decoder I

- Presorting help in generating reduced deviation path Δ_R.
- Generated on spot offline using cost function.
- Each deviation path has a cost

$$\xi(\delta) = \sum_{j=0}^{d_c-1} \delta(j) + (3 \cdot j),\ \delta(j) \neq 0,\ \forall\ \delta \in \Delta. \tag{10}$$

- Any deviation path $\delta \in \Delta$ with cost $\xi(\delta)$ higher than ξ_{max} is omitted.

Presorted SYN-BRD Decoder II

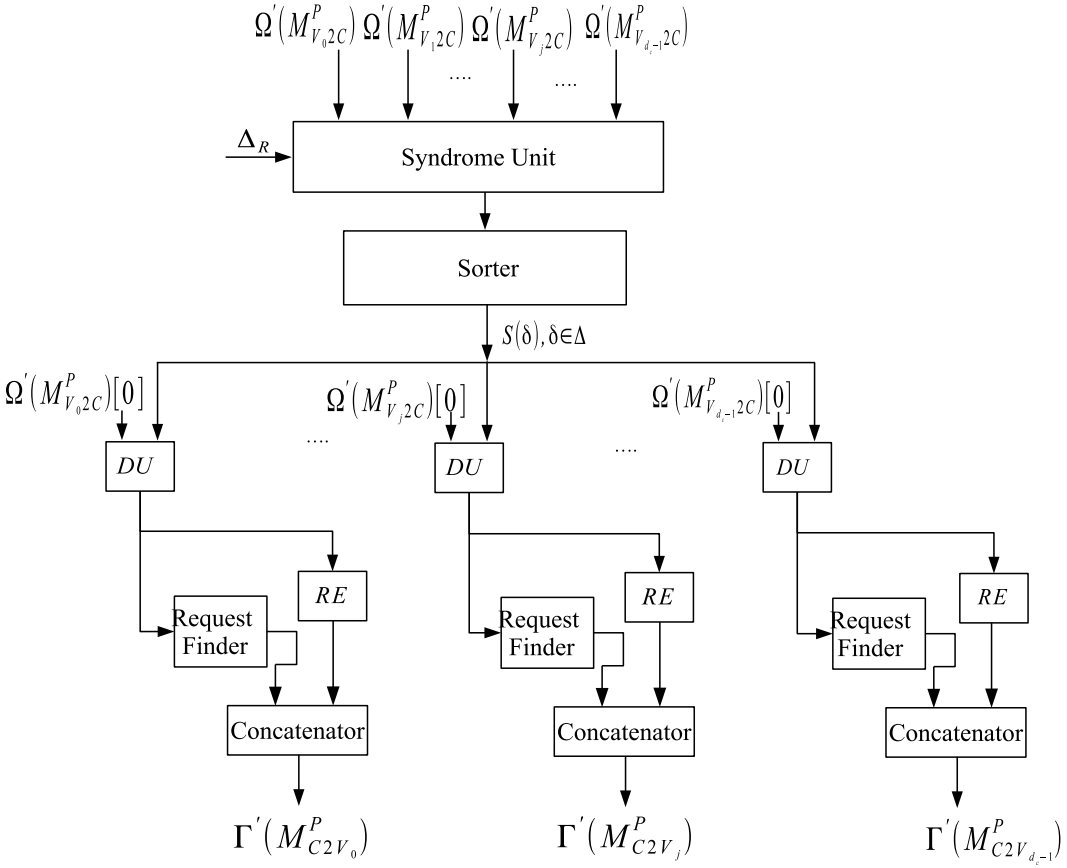


Figure 48: Structure of Presorted SYN-BRD Decoder

Syndrome-based BRD I

SYN-BRD for $d_c = 12$ ($r = 5/6$) on GF(64).

- Size of variable-to-check message: $n_{vc} = 5$.
- Size of best candidates: $n_B = 4$.
- Size of requested candidates: $n_R = 3$.

Decoder	Input size	Output size	Syndromes
SYN-EMS	(16,15)	(16,15)	456
SYN-BRD	(5,4)	(4,6)	313
Presorted SYN-BRD	(5,4)	(4,6)	220

Syndrome-based BRD II

SYN-BRD for $d_c = 3$ ($r = 1/3$) on GF(64)

- Size of variable-to-check message: $n_{vc} = 14$.
- Size of best candidates: $n_B = 7$.
- Size of requested candidates: $n_R = 8$.

Decoder	Input size	Output size	Syndromes
SYN-EMS	(20,19)	(20,19)	70
SYN-BRD	(14,13)	(6,14)	67
Presorted SYN-BRD	(14,13)	(6,14)	55

Syndrome-based BRD III

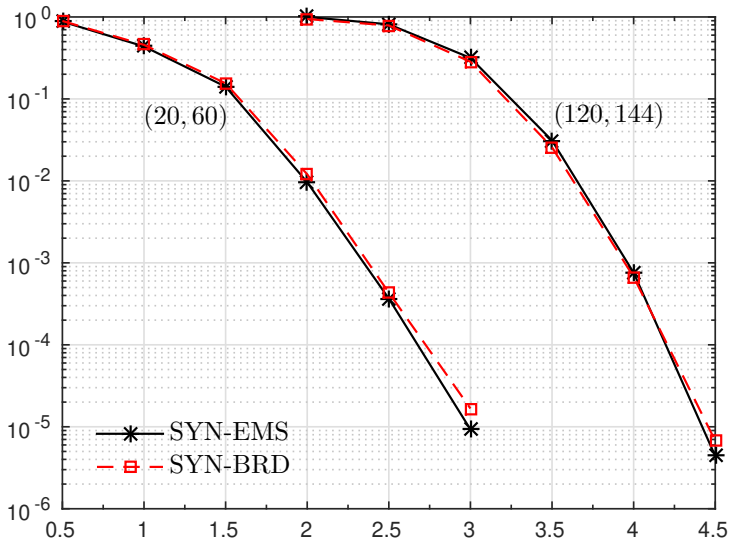


Figure 49: SYN-BRD Decoder Simulation for (K, N) symbols

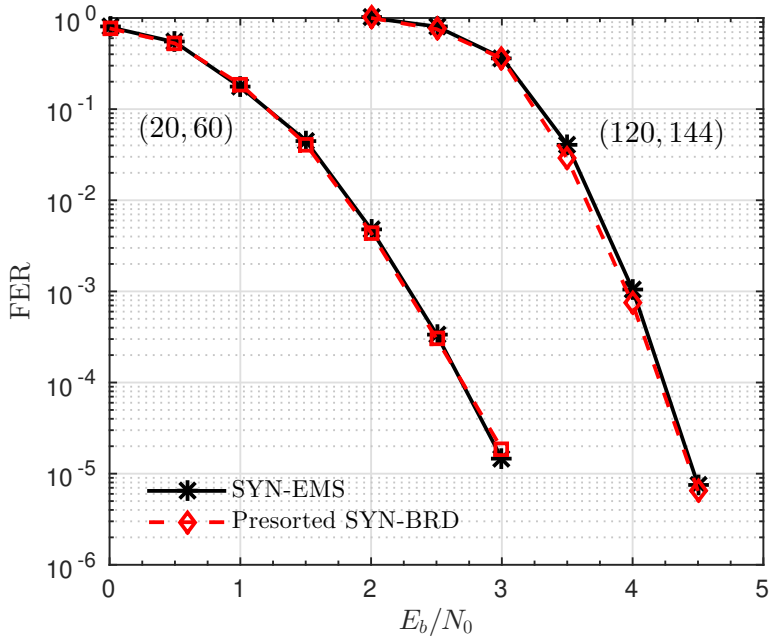


Figure 50: Simulation Results of Presorted SYN-BRD Decoder

FB-BRD I

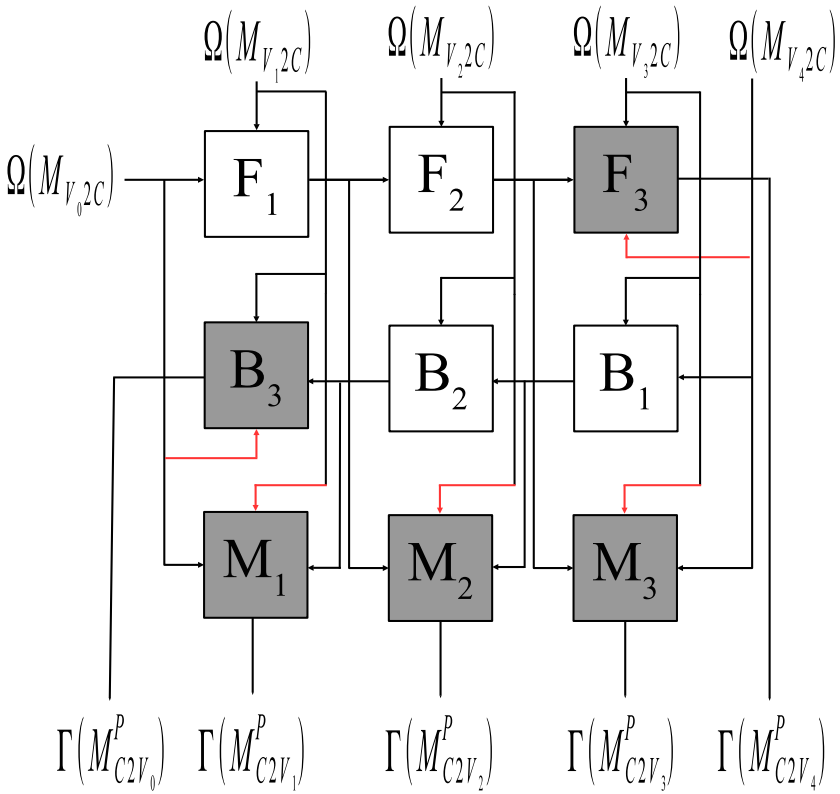


Figure 51: Forward-Backward BRD Architecture for $d_c = 5$

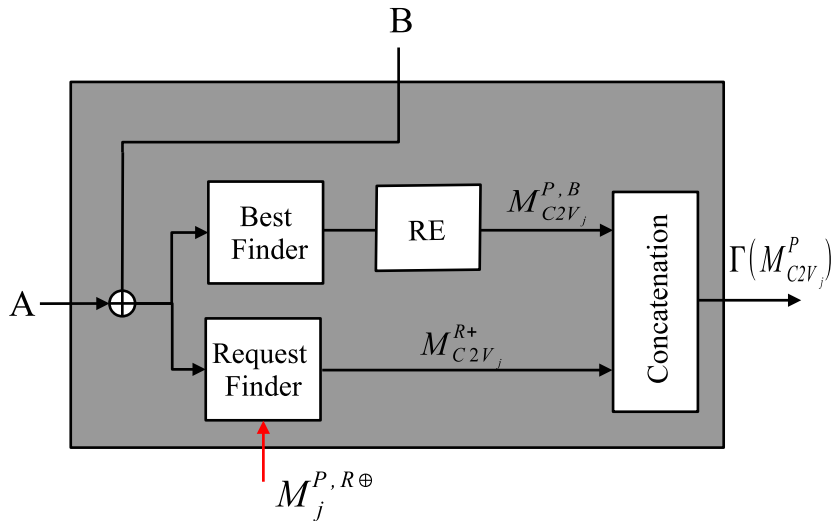


Figure 52: Internal Structure of BRD-ECN

Presorted FB-BRD I

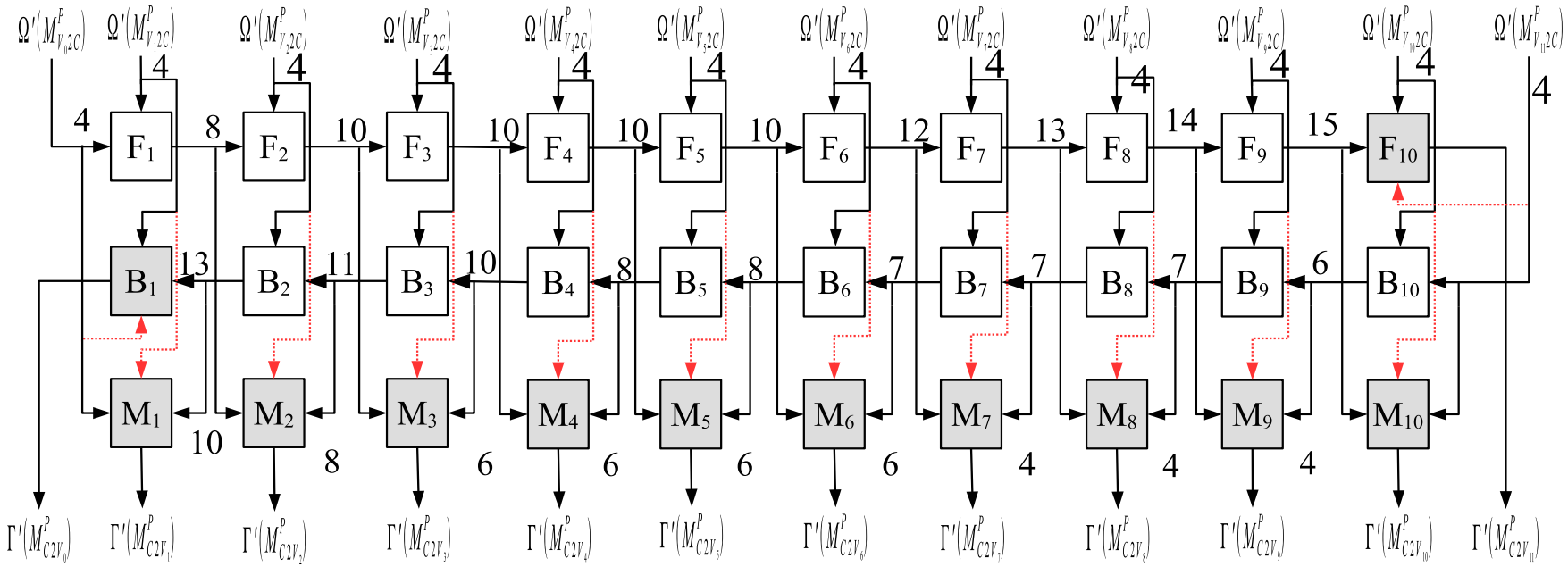


Figure 53: Structure of the Presorted FB-BRD for $N = 144, K = 120$.

Presorted FB-BRD II

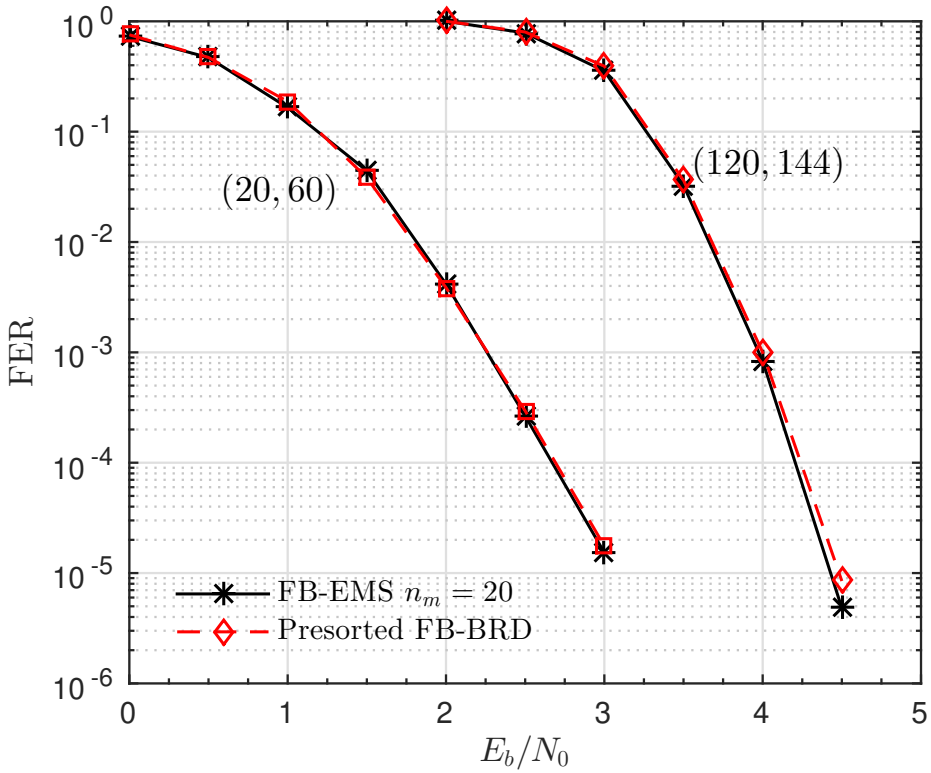


Figure 54: Simulation Performance of Presorted FB-BRD for $r = 1/3$ and $r = 5/6$.

Implementation of BRD-CN I

$$T = \frac{200 \text{ MHz} \times 864 \text{ bits}}{5 \text{ iterations} \times 144 \text{ bits} \times 10 \text{ CC}} = 24 \text{ Mbps}. \tag{11}$$

Implementation of BRD-CN II

- Best Finder: Generates n_B best candidates.
- Request Finder: Finds n_R LLRs of requested symbols.

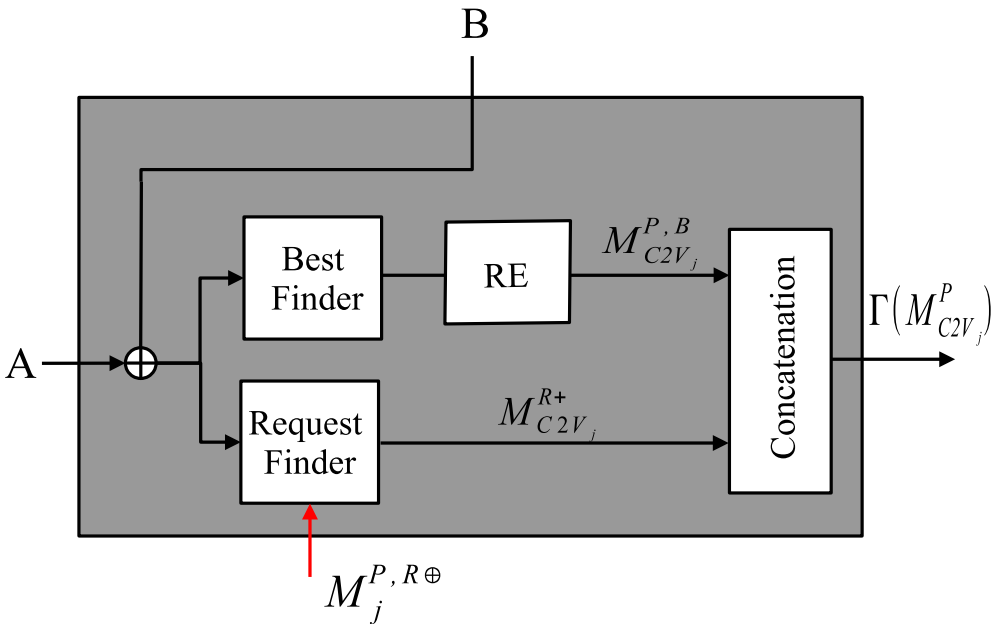


Figure 55: BRD-ECN Internal Structure

Implementation of BRD-CN III

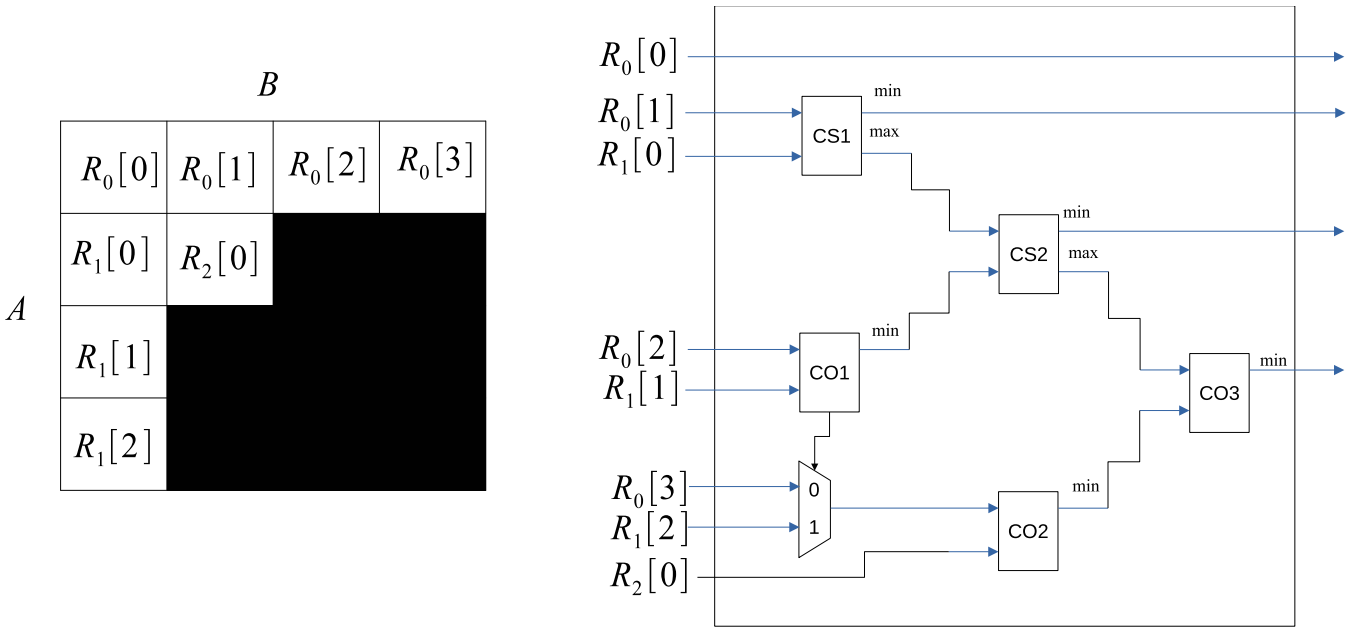


Figure 56: Internal Structure of Best Finder.

Implementation of BRD-CN IV

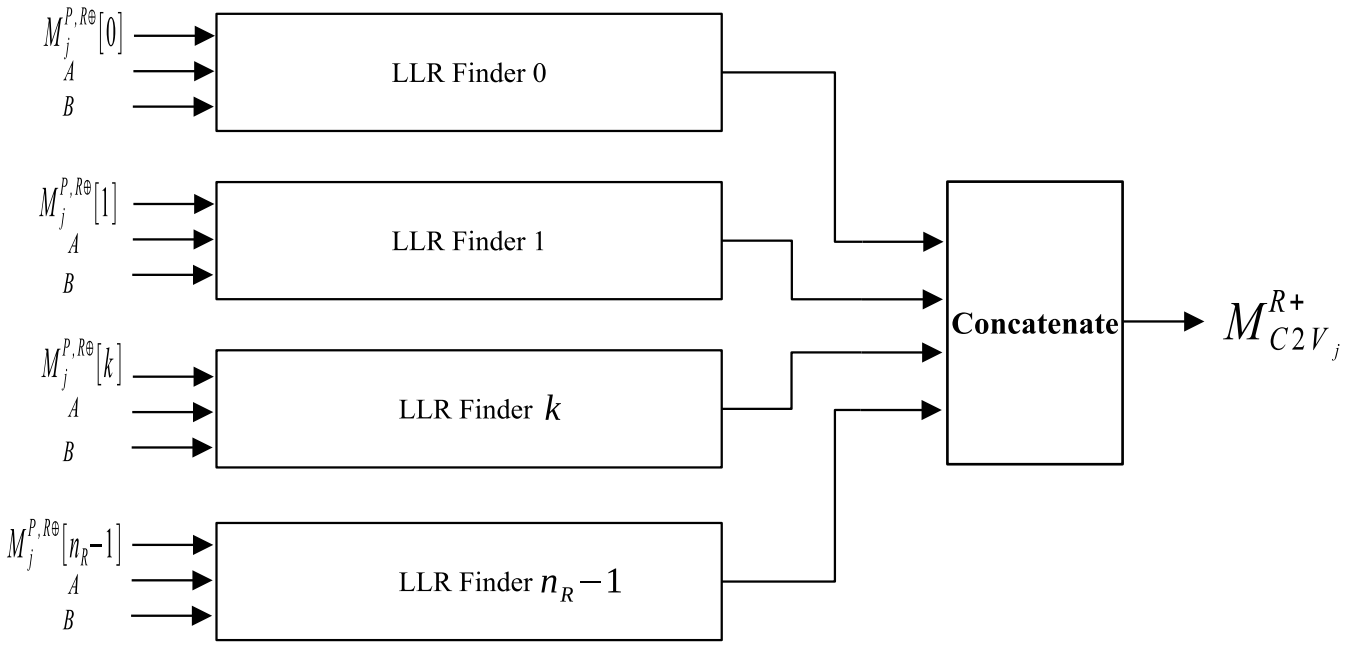


Figure 57: Internal Structure of Request Finder Block.

Implementation of BRD-CN V

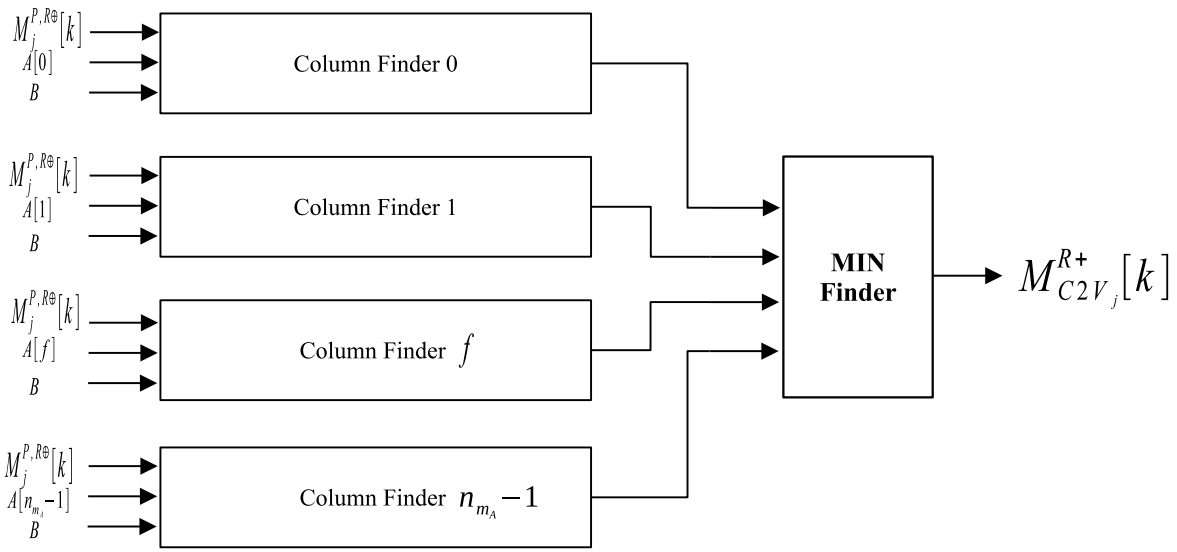


Figure 58: Internal Structure of LLR Finder Block.

Implementation of BRD-CN VI

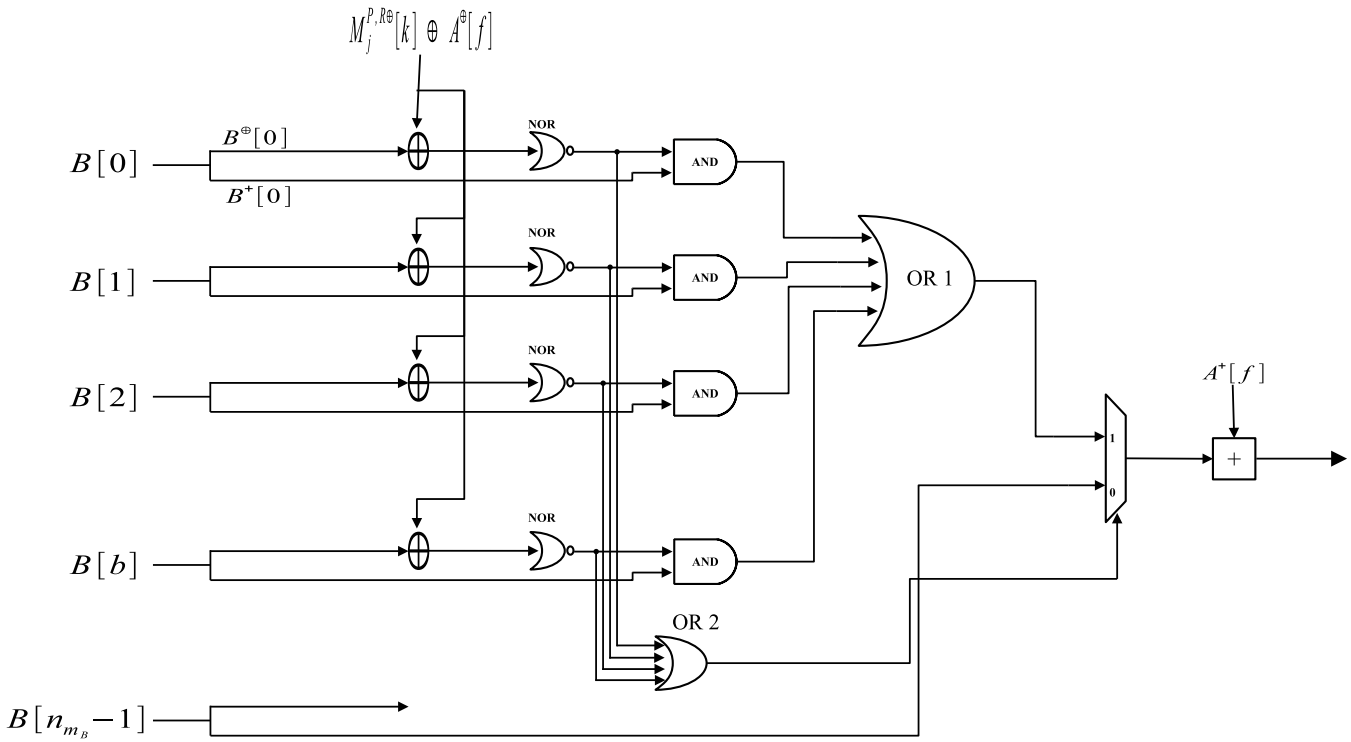


Figure 59: Internal Structure of Column Finder Block.

Input/Output Sizes in SC-PA. I

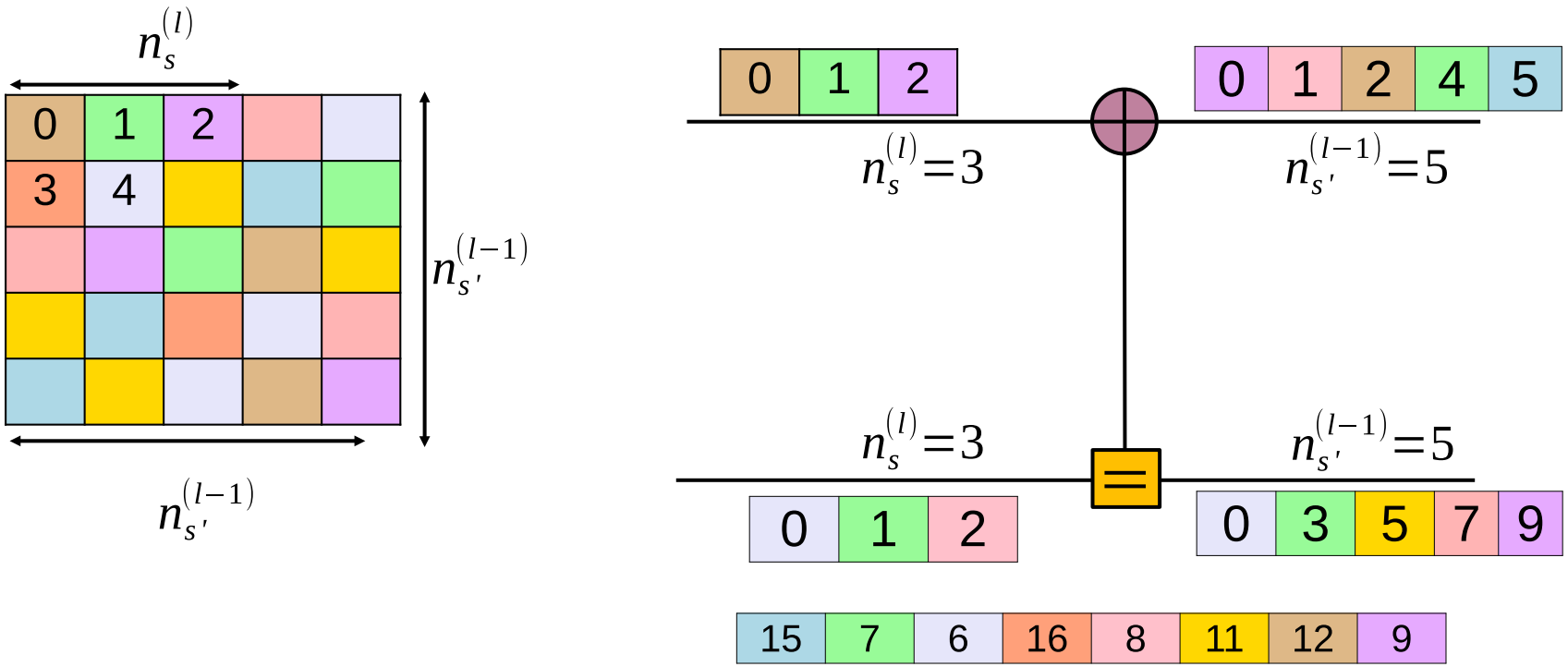


Figure 60: Input/Output of Kernel Nodes.

Input/Output Sizes in SC-PA. II

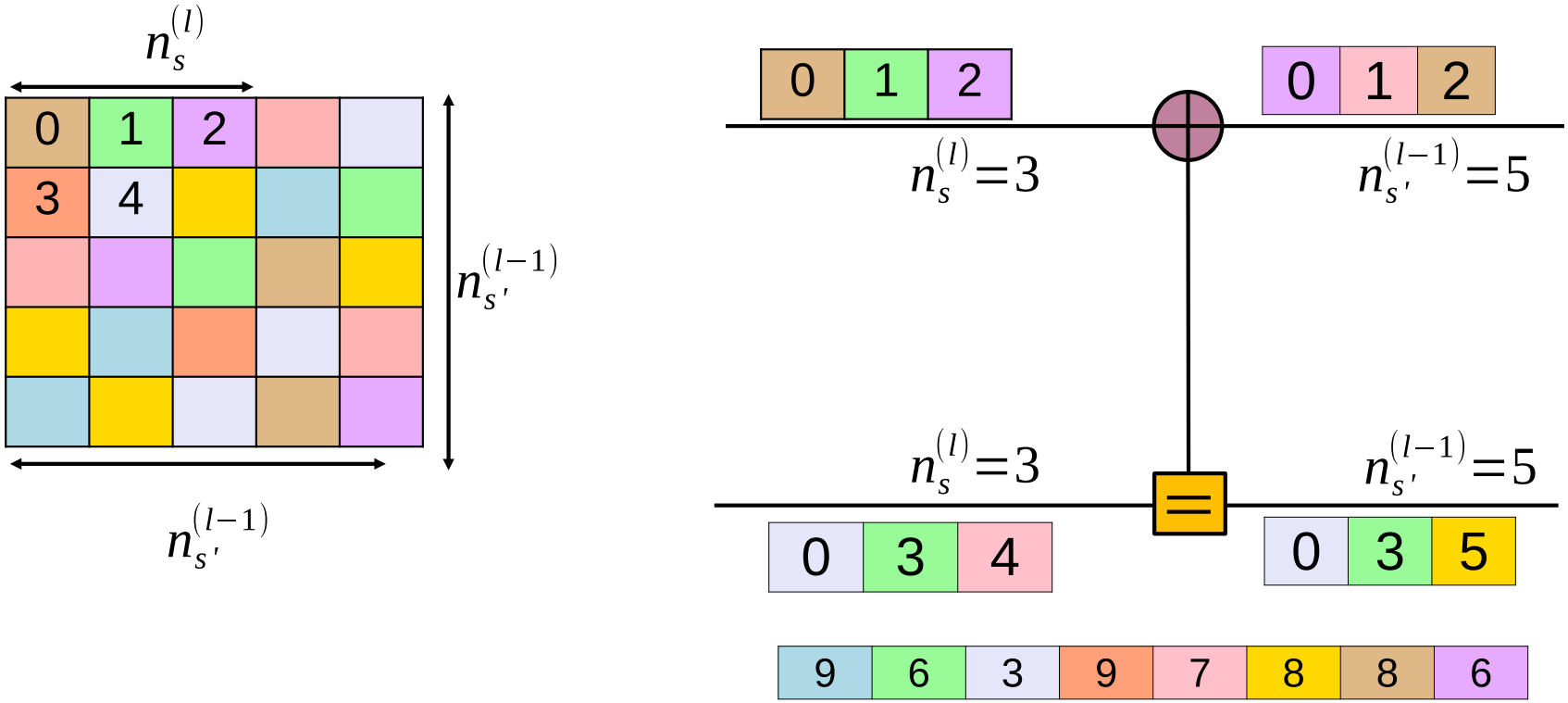


Figure 61: Input/Output of Kernel Nodes.

CCSK Modulation for SC-PA

- B1-SCL32: Binary SCL Decoder with $L = 32$
  - $K_b = K.p.$
  - $N_b = N.q.$
- B1-SCL32: Binary SCL Decoder with $L = 32$
  - $K_b = K.p.$
  - $N_b = N.p.$
  - Repetition code of p/q.

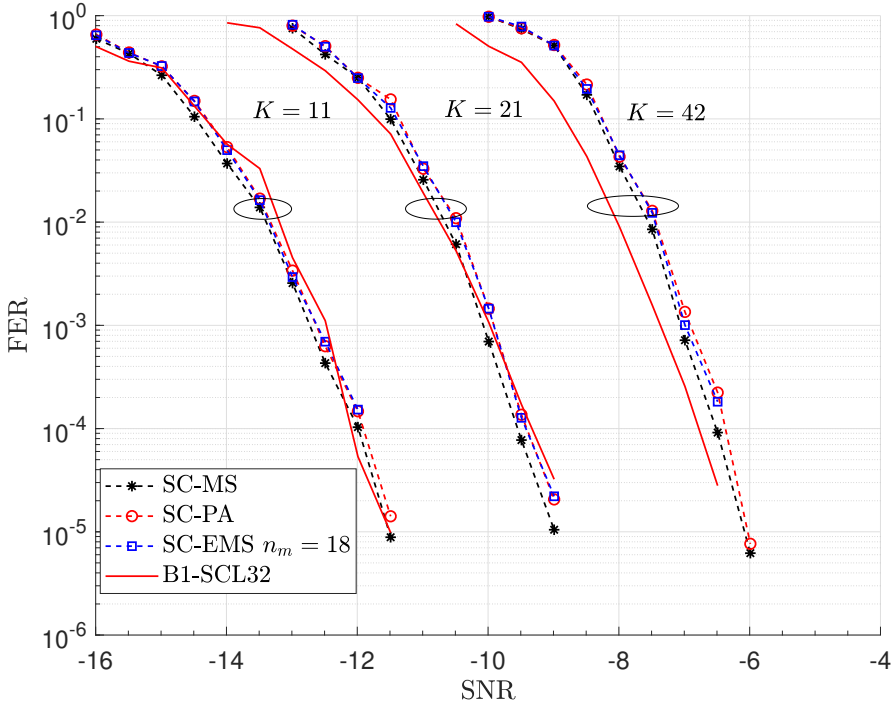


Figure 62: Simulation Results for $N = 64$ over GF(64).

Bibliography I

[1] K. Saied. (2019), "Quasi Cyclic Small Packet," [Online]. Available: https://qcsp.univ-ubs.fr.

[2] G. Dillard, M. Reuter, J. Zeiddler, and B. Zeidler, "Cyclic Code-Shift Keying: A Low Probability of Intercept Communication Technique," *IEEE Transactions on Aerospace and Electronic Systems*, 2003.

[3] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[4] S. P. et al., "Performance evaluation of non-binary ldpc codes on wireless channels," in *ICT-MobileSummit 2009 Conference Proceedings*, 2009, ISBN: 978-1-905824-12-0.

[5] C. S. N. Office. (2019), "BeiDou Navigation Satellite System Signal In Space Interface Control Document," [Online]. Available: http://www.beidou.gov.cn/xt/gfxz/201912/P020230516558050038035.pdf.

[6] R. Gallager, *Low Density Parity-Check Codes*. Cambridge MA: MIT Press, 1963.

[7] D. MacKay, "Near shannon limit performance of low density parity check codes," English, *Electronics Letters*, vol. 32, 1645–1646(1), 18 Aug. 1996, ISSN: 0013-5194. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/el_19961141.

[8] ——, "Good error-correcting codes based on very sparse matrices," in *Proceedings of IEEE International Symposium on Information Theory*, 1997, pp. 113–. DOI: 10.1109/ISIT.1997.613028.

[9] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $(2,d_c)$-LDPC codes over GF(q) using their binary images," *IEEE Transactions on Communications*, vol. 56, no. 10, pp. 1626–1635, 2008. DOI: 10.1109/TCOMM.2008.060527.

[10] B. Liu, J. Gao, G. Dou, and W. Tao, "Weighted symbol-flipping decoding for nonbinary ldpc codes," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 1, 2010, pp. 223–226. DOI: 10.1109/NSWCTC.2010.59.

[11] V. Savin, "Min-Max Decoding for Non-binary LDPC Codes," in *2008 IEEE International Symposium on Information Theory*, 2008, pp. 960–964. DOI: 10.1109/ISIT.2008.4595129.

Bibliography II

[12] M. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Transactions on Communications*, vol. 47, no. 5, pp. 673–680, 1999. DOI: 10.1109/26.768759.

[13] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, "Low-complexity, low-memory ems algorithm for non-binary ldpc codes," in *2007 IEEE International Conference on Communications*, 2007, pp. 671–676. DOI: 10.1109/ICC.2007.115.

[14] P. Schläfer, N. Wehn, M. Alles, T. Lehnigk-Emden, and E. Boutillon, "Syndrome-based Check Node Processing of High Order NB-LDPC Decoders," in *2015 22nd International Conference on Telecommunications (ICT)*, 2015, pp. 156–162.

[15] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, "Low-complexity Decoding for Non-Binary LDPC Codes in High Order Fields," *IEEE Transactions on Communications*, vol. 58, no. 5, pp. 1365–1375, 2010.

[16] E. Boutillon and L. Conde-Canencia, "Simplified check node processing in nonbinary LDPC decoders," in *2010 6th International Symposium on Turbo Codes Iterative Information Processing*, 2010, pp. 201–205. DOI: 10.1109/ISTC.2010.5613839.

[17] O. Abassi, L. Conde-Canencia, A. Al Ghouwayel, and E. Boutillon, "A Novel Architecture for Elementary-Check-Node Processing in Nonbinary LDPC Decoders," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 2, pp. 136–140, 2017. DOI: 10.1109/TCSII.2016.2551550.

[18] E. Li, K. Gunnam, and D. Declercq, "Trellis-Based Extended Min-Sum for Decoding Non-Binary LDPC Codes," in *2011 8th International Symposium on Wireless Communication Systems*, 2011, pp. 46–50.

[19] J. Tian, S. Song, J. Lin, and Z. Wang, "Efficient T-EMS Based Decoding Algorithms for High-Order LDPC Codes," *IEEE Access*, vol. 7, pp. 50 980–50 992, 2019.

[20] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009. DOI: 10.1109/TIT.2009.2021379.

[21] F. Cochachin, L. Luzzi, and F. Ghaffari, "Reduced Complexity of a Successive Cancellation Based Decoder for NB-Polar Codes," in *2021 11th International Symposium on Topics in Coding (ISTC)*, 2021.

[22] F. Cochachin and G. Fakhreddine, "A Lightweight Encoder and Decoder for Non-Binary Polar Codes," in *2023 22nd International Conference on Wireless Networks (ICWN)*, 2023.

Bibliography III

[23] P. Chen, B. Bai, and X. Ma, "Non-Binary Polar Coding with Low Decoding Latency and Complexity," *Journal of Information and Intelligence*, 2022, ISSN: 2949-7159.

[24] J. Jabour, C. Marchand, and E. Boutillon, "The Best, The Requested, and The Default Non-Binary LDPC Decoding Algorithm," in *2021 11th International Symposium on Topics in Coding (ISTC)*, 2021, pp. 1–5. DOI: 10.1109/ISTC49272.2021.9594148.

[25] ——, "The Best, the Requested, and the Default Elementary Check Node for EMS NB-LDPC Decoder," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, 2023, pp. 1–6. DOI: 10.1109/WCNC55385.2023.10118720.

[26] J. Jabour, A. C. Al-Ghouwayel, and E. Boutillon, "Asymmetrical Extended Min-Sum for Successive Cancellation Decoding of Non-Binary Polar Codes," in *2023 12th International Symposium on Topics in Coding (ISTC)*, 2023, pp. 1–5. DOI: 10.1109/ISTC57237.2023.10273502.

[27] ——, "Polarization-Aware Decoding for Non-binary Polar Decoders," *IEEE Communication Letters*, 2023. DOI: Submitted.

[28] E. Boutillon, J. Jabour, and M. Cédric, "A method for decoding a codeword encoded using a non-binary code, corresponding device, and computer program," WO2023025960A1, 2023. [Online]. Available: https://patents.google.com/patent/WO2023025960A1.

[29] E. Boutillon and L. Conde-Canencia, "Bubble check: a simplified algorithm for elementary check node processing in Extended Min-Sum non-binary LDPC decoders," *IEE Electronics Letters*, vol. 46, no. 9, pp. 633–631, 2010.

[30] C. Marchand and E. Boutillon, "NB-LDPC check node with pre-sorted input," in *2016 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*, 2016, pp. 196–200. DOI: 10.1109/ISTC.2016.7593104.

[31] H. Harb, C. Marchand, A. A. Ghouwayel, L. Conde-Canencia, and E. Boutillon, "Pre-Sorted Forward-Backward NB-LDPC Check Node Architecture," in *2016 IEEE International Workshop on Signal Processing Systems (SiPS)*, 2016, pp. 142–147. DOI: 10.1109/SiPS.2016.33.