Reduction of complexity for Non-binary LDPC decoders with compressed messages

Jesús O. Lacruz, Francisco García-Herrero and Javier Valls, Member IEEE

Abstract

In this paper a method to compress the messages between the check nodes and the variable nodes is proposed. This method is named as compressed non-binary message-passing (CNBMP). The CNBMP reduces the number of messages exchanged between one check node and the connected variable nodes from $d_c \times q$ to $5 \times q$, and its application has a high impact in the performance of the decoder: the storage and routing area is reduced and the throughput is increased. Unlike other methods, the CNBMP does not introduce any approximation or modification in the information and the processed operations are exactly the same as the original decoders, hence, no performance degradation is introduced. To demonstrate its advantages, an architecture applying this CNBMP to the Trellis Min-max algorithm was derived showing that most of the storage resources were also reduced from $d_c \times q$ to $5 \times q$. This architecture was implemented for a (837,726) NB-LDPC code using a 90nm CMOS technology reaching a throughput of 981Mbps with an area of 10.67$mm^2$, which is 3.9 more efficient than the best solution found in literature.

Index Terms

LDPC codes, decoding, non-binary, hardware implementation, high-throughput

I. INTRODUCTION

The two main bottlenecks of non-binary low-density parity-check (NB-LDPC) decoder architectures are the storage resources and the maximum throughput. Regardless their significant benefits, such as a better behaviour in the error floor region and a more robust correction for burst

F. García, and J. Valls are with the Instituto de Telecomunicaciones y Aplicaciones Multimedia, at Universitat Politècnica de València, 46730 Gandia, Spain (e-mail: fragarh2@epsg.upv.es, jvalls@eln.upv.es).

J. Lacruz is with the Electrical Engineering Department, Universidad de Los Andes, Mérida, 5101, Venezuela. (e-mail: jlacruz@ula.ve)
errors, NB-LDPC codes cannot compete with their binary counterparts in terms of complexity or throughput/area efficiency.

Several alternatives to the original Q-ary Sum-of-Product algorithm (QSPA) [1] were proposed during this last decade in order to keep the best correction performance possible and reduce complexity. The most remarkable ones are the Extended Min-Sum (EMS) [2] and Min-Max (MM) [3] algorithms, which reduced the complexity of the check node processor and the storage resources. However, a parallel implementation of these algorithms was prohibitive in terms of wiring between check node and variable node processors and arithmetic resources. For this reason all the architectures derived from these two algorithms applied the forward-backward metrics, which consist in a serial computation of the check node information. All the decoders based on the forward-backward suffer from a very large number of clock cycles per iteration, limiting the maximum throughput to a few Mbps [4].

In order to increase the degree of parallelism keeping the same error correction, a new version of the EMS algorithm named as Trellis-EMS (T-EMS) was proposed in [5]. This method allowed hardware designers to implement a fully parallel check node in a layered architecture [6]. This implementation did not sacrifice efficiency in terms of throughput/area compared to other serial implementations based on trellis [7] and increased throughput more than three times. Further improvements were introduced with the Trellis Min-max (TMM) in [8]. Despite this, the decoder from [8] required 14.7\(mm^2\) of area with a 90nm CMOS process and reached a throughput of 660Mbps, which is far from the results of modern binary LDPC decoders for the same technology (9.6\(mm^2\), 45.42Gbps) [9]. While the binary architectures just exchange a number of messages equal to the degree of the check node \((d_c)\) between check node and variable node, non-binary decoders require \(q\) times more wires/connections; and the same happens for the memories and registers, which are about the 80\% of the decoder’s area.

In this brief a method to reduce the number of messages exchanged in non-binary decoders between the check node and the variable node is introduced. This method does not vary the computation of the decoding algorithm nor reduces the information transferred between nodes, so it does not introduce any performance degradation. This proposal compresses the information transmitted in the message passing reducing the size of the messages from \(d_c \times q\) to \(5 \times q\). This has a great impact in both area and throughput specially for high rate codes. As an example, an implementation for the same code as in [8] and [7] achieves 981Mbps of throughput with an area of 10.6\(mm^2\) for a 90nm CMOS process.
The rest of the paper has four sections. Section II includes a summary of the NB-LDPC message-passing of the decoding algorithms. Section III describes the proposal of this work. Section IV shows the impact of the new message-passing in a hardware implementation and compares the results to other existing architectures. Section V outlines the conclusions.

II. NON-BINARY LDPC MESSAGE PASSING

Let $H$ be the $M \times N$ parity check matrix with coefficients $h_{i,j} \in GF(q)$ that defines an $(N,K)$ NB-LDPC code. $\mathcal{N}(m)$ and $\mathcal{M}(n)$ are described as the sets that consist of all the non-zero elements of a row $m$ (check node) and a column $n$ (variable node) respectively. The size of the sets $\mathcal{N}(m)$ and $\mathcal{M}(n)$ are the degree of check node ($d_c$) and the degree of variable node ($d_v$). The $d_c$ and $d_v$ degrees represent the number of messages that each check node and variable node receive respectively. The set of messages from check node to variable node are denoted as $R$ and the set of messages from variable node to check node are $Q$. Each of these messages consists of $q$ elements, due to the fact of performing operations over $GF(q)$. The method to compute each of these sets depends on the decoding algorithm applied. The algorithms that provide a better performance with lower complexity are T-EMS and T-MM, which have a different processing at the check node but share the same operations at the variable node. To a better understanding of the message-passing between check node and variable node, a short explanation of the basics operations performed in the check node is included next, for more details about the different decoding processes we refer to [5] and [8].

In addition, to perform a parallel processing of the check node we will assume delta domain [5], [6] messages as inputs and outputs at the check node.

Let $\Delta Q$ be the set of $d_c$ messages from the variable node in delta domain defined as:

$$\Delta Q = \{\Delta Q_{m,n} \mid n \in \mathcal{N}(m), m \in \mathcal{M}\}$$  \hspace{1cm} (1)

Each element $\Delta Q_{m,n}$ includes the likelihood of being the symbol $\alpha^x \in GF(q)$, $x = \{-\infty, 0, 1, \ldots, q-2\}$:

$$\Delta Q_{m,n} = \{Q_{m,n}(\alpha^{-\infty}), Q_{m,n}(\alpha^0), \ldots, Q_{m,n}(\alpha^{q-2})\}$$  \hspace{1cm} (2)

The output messages of the check node in the delta domain are also of length $d_c$:

$$\Delta R = \{\Delta R_{m,n} \mid n \in \mathcal{N}(m), m \in \mathcal{M}\}$$  \hspace{1cm} (3)
The likelihood of each symbol to accomplish the parity check equation of the check node is defined as:

$$\Delta R_{m,n} = \{ \Delta R_{m,n}(\alpha^{-\infty}), \Delta R_{m,n}(\alpha^0), \ldots, \Delta R_{m,n}(\alpha^{q-2}) \}$$ (4)

To compute the reliability of each one of the $q$ symbols in a single message, the check node update equations consider the combinations of the most reliable input messages. If only the two most reliable messages per symbol are considered the update rules for the check node follow the next conditions:

i) If the input likelihood of the symbol $\alpha^x$ for the edge $\{m, n\}$ is not the most reliable for $\alpha^x$ nor is considered to compute other $\alpha^y$ output message, $\Delta R_{m,n}(\alpha^x)$ is equal to the most reliable value $Q_{m,n_0}(\alpha^x)$:

$$\Delta R_{m,n}(\alpha^x) = \{\text{min}(Q_{m,n_0}(\alpha^x), Q_{m,n_0}(\alpha^y) + Q_{m,n_0}(\alpha^z))\},$$

$$\alpha^y + \alpha^z = \alpha^x, \forall \alpha^y, \alpha^z \in GF(q) \leftrightarrow$$

$$[Q_{m,n}(\alpha^x) \neq Q_{m,n_0}(\alpha^x)] \cap [Q_{m,n_0}(\alpha^x) + Q_{m,n_0}(\alpha^z) \neq$$

$$\Delta R_{m,n}(\alpha^y)], \alpha^x + \alpha^z = \alpha^y, \forall \alpha^y, \alpha^z \in GF(q)$$ (5)

Being $Q_{m,n_0}(\alpha^x)$ and $Q_{m,n_1}(\alpha^x)$:

$$Q_{m,n_0}(\alpha^x) \leq Q_{m,n_1}(\alpha^x) \leq Q_{m,n}(\alpha^x), \forall n \in N(m) \setminus \{n_0, n_1\}$$ (6)

ii) If the input likelihood of the symbol $\alpha^x$ for the edge $\{m, n\}$ is the most reliable for $\alpha^x$, $\Delta R_{m,n}(\alpha^x)$ takes the value of the second more reliable message:

$$\Delta R_{m,n}(\alpha^x) = \{Q_{m,n_1}(\alpha^x)\} \leftrightarrow [Q_{m,n}(\alpha^x) = Q_{m,n_0}(\alpha^x)]$$ (7)

iii) If the input likelihood of the symbol $\alpha^x$ for the edge $\{m, n\}$ is involved in the output reliability of $\alpha^y$, $\Delta R_{m,n}(\alpha^x)$ takes the value of the most reliable message $Q_{m,n_0}(\alpha^x)$:

$$\Delta R_{m,n}(\alpha^x) = \{Q_{m,n_0}(\alpha^x)\} \leftrightarrow [Q_{m,n_0}(\alpha^x) + Q_{m,n_0}(\alpha^z) =$$

$$= \Delta R_{m,n}(\alpha^y)], \alpha^x + \alpha^z = \alpha^y, \forall \alpha^y, \alpha^z \in GF(q)$$ (8)

To reduce the number of operations at the check node and share results a set that includes common computation was proposed in [5], and defined as:

$$P_m = \{P_m(\alpha^{-\infty}), P_m(\alpha^0), \ldots, P_m(\alpha^{q-2})\}, m \in M$$ (9)
Where each element from the set $P_m$ includes the two most reliable input values from $\alpha^x$:

$$P_m(\alpha^x) = \{P_{m_0}(\alpha^x) = Q_{m,n_0}(\alpha^x), P_{m_1}(\alpha^x) = Q_{m,n_1}(\alpha^x)\} \quad (10)$$

Based on the set $P_m$ an extra set is computed in [5]. This set includes the values from $\triangle R_{m,n}(\alpha^x)$ in equation (5). The set is defined as follows:

$$E_m = \{E_m(\alpha^{-\infty}), E_m(\alpha^0), \ldots, E_m(\alpha^{q-2})\}, \ m \in M \quad (11)$$

$$E_m(\alpha^x) = \{\min(Q_{m,n_0}(\alpha^x), Q_{m,n_0}(\alpha^y) + Q_{m,n_0}(\alpha^z))\}$$

$$(\alpha^y + \alpha^z = \alpha^x \in GF(q)) \bigwedge (Q_{m,n_0}(\alpha^y) + Q_{m,n_0}(\alpha^z) < Q_{m,n_0}(\alpha^a) + Q_{m,n_0}(\alpha^b), \ \alpha^a + \alpha^b = \alpha^x, \ \forall \alpha^a, \alpha^b \in GF(q) \setminus \{\alpha^y, \alpha^z\}) \quad (12)$$

Regardless the definition of the extra set the output messages of the check node are $\triangle R_{m,n}$, which is a set of size $q \times d_c$.

### III. Compressed Non-Binary Message-Passing (CNBMP)

With the aim of reducing the size of the sets that conform the messages shared between check node and variable node we propose a new ordering of the information. With these new sets the number of information exchanged between check node and variable node is reduced considerably and the set $\triangle R_{m,n}$ is easily derived at the variable node. We name this method Compressed Non-Binary Message-Passing (CNBMP).

First we define the set $C_m$ as follows:

$$C_m = \{C_m(\alpha^{-\infty}), C_m(\alpha^0), \ldots, C_m(\alpha^{q-2})\}, \ m \in M \quad (13)$$

$$C_m(\alpha^x) = \{N_{x'}(m)\} \quad (14)$$

Each $N_{x'}(m)$ element contains the index $n$ of the edge $\{m, n\}$ for the symbol $\alpha^x$ in which $\triangle R_{m,n}$ is not updated following equation (5):

$$N_{x'}(m) = \{n_0\} \leftrightarrow (\alpha^x \in GF(q)) \bigwedge (Q_{m,n_0}(\alpha^x) = E_m(\alpha^x)) \bigvee (\alpha^x + \alpha^z = \alpha^y, \forall \alpha^y, \alpha^z \in GF(q)) \bigwedge Q_{m,n_0}(\alpha^x) + Q_{m,n_0}(\alpha^z) = E_m(\alpha^y)) \quad (15)$$
Considering that the sets $E_m$ and $P_m$ are computed the message $\Delta R_{m,n}$ can be recovered at the variable node following the next equations:

$$\Delta R_{m,n}(\alpha^x) = E_m(\alpha^x), \ n \in N(m) \setminus N_x(m)$$  

$$\Delta R_{m,n}(\alpha^x) = P_{m1}(\alpha^x) \leftrightarrow P_{m0}(\alpha^x) = E_m(\alpha^x), \ n \in N_x(m)$$  

$$\Delta R_{m,n}(\alpha^x) = P_{m0}(\alpha^x) \leftrightarrow P_{m0}(\alpha^x) \neq E_m(\alpha^x), \ n \in N_x(m)$$

It is important to remark that: i) whether CNBMP is applied or not the sets $P_m$ and $E_m$ are computed because of computational efficiency [5], so we are not adding any extra operation; and ii) it can be demonstrated that the value of the messages $\Delta R_{m,n}$ are exactly the same applying equations (5) to (8) or (16) to (18), so in terms of error correction performance we can claim that CNBMP is equivalent to the original T-EMS or T-MM algorithms as it does not include any approximation.

Note that applying the CNBMP the output information of the check node is conformed by the set $E_m$ that contains $q$ elements and the sets $C_m$ and $P_m$ that contain $2 \times q$ elements each one. So in total the cardinality of the output information is $5 \times q$, unlike previous proposals found in literature.

To sum up, the check node with the CNBMP does not compute equations (5) to (8), but equations (16) to (18). In addition, the message passing consists of the sets $C_m$, $P_m$ and $E_m$, not of $\Delta R_{m,n}$, which is of size $d_c \times q$, as shown in Fig.1.

### IV. Hardware Impact of CNBMP

The first improvement for the hardware architectures of NB-LDPC decoders is the reduction of the wiring. According to the implementation reports, the maximum frequency of the decoder is not limited by the depth of the logic gates, but for the length of the wiring and the routing congestion. So, if we apply CNBMP, the wires between both check node and variable node processors will be reduced and hence, routing congestion will be mitigated. The reduction is

$$\lambda = (d_c \times q \times Q_b)/(3 \times q \times Q_b + 2 \times q \times \lceil \log_2(d_c) \rceil)$$  

(Fig.2), assuming that the messages at the check node are quantized with $Q_b$ bits and that the set $C_m$ requires $\lceil \log_2(d_c) \rceil$ bits to represent the indexes $n$. As it is shown next with this reduction of the routing there is an improvement in the maximum frequency.
Fig. 1. i) Check node without CNBMP ii) Check node with CNBMP

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantization ($Q_b$)</td>
<td>5 bits</td>
<td>7 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>7 bits</td>
<td>6 bits</td>
<td>6 bits</td>
</tr>
<tr>
<td>Gate Count (NAND)</td>
<td>1.29M</td>
<td>8.51M</td>
<td>2.1M</td>
<td>871K</td>
<td>2.75M</td>
<td>3.28M</td>
<td>0.9M / 1.25M</td>
</tr>
<tr>
<td>$f_{clk}$ (MHz)</td>
<td>200</td>
<td>250</td>
<td>500</td>
<td>200</td>
<td>250</td>
<td>238</td>
<td>333 / 300</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>64</td>
<td>223</td>
<td>64</td>
<td>66</td>
<td>484</td>
<td>660</td>
<td>1089 / 981</td>
</tr>
<tr>
<td>Throughput (Mbps) 90 nm</td>
<td>149</td>
<td>223</td>
<td>107</td>
<td>154</td>
<td>484</td>
<td>660</td>
<td>1089 / 981</td>
</tr>
<tr>
<td>Efficiency 90 nm (Mbps/M-gates)</td>
<td>115.5</td>
<td>26.2</td>
<td>50.9</td>
<td>176.8</td>
<td>176</td>
<td>201</td>
<td>1210 / 784.8</td>
</tr>
<tr>
<td>Area (mm$^2$)</td>
<td>-</td>
<td>46.18</td>
<td>-</td>
<td>-</td>
<td>19</td>
<td>14.75</td>
<td>10.4 / 10.6</td>
</tr>
</tbody>
</table>
The second improvement is in terms of storage resources. To perform the layered schedule the decoder requires the storage, in registers or memories, of the information from the check node in the previous iteration, in order to compute the extrinsic information. Therefore, \( M \) addresses of depth equal to the size of the output messages from the check node are required. As it is previously explained, the number of the output messages without CNBMP is \( d_c \times q \times Q_b \) and the number with CNBMP is equal to \( 3 \times q \times Q_b + 2 \times q \times \lceil \log_2(d_c) \rceil \), so the reduction in storage resources is also \( \lambda \) (Fig.2). Note that applying CNBMP will be specially advantageous for high rate codes, where \( d_c \) is very large. However, even with low and medium rate codes there will be significant improvements, as far as the only requirement to get some complexity reduction is that \( d_c > 5 \). To de-compress the messages at the variable node comparators and multiplexors implement the conditions from equations (16) to (18) to select whether \( E_m(\alpha^x) \) or \( P_{mx}(\alpha^x) \) and
$P_{m_1}(\alpha^x)$ is applied to update $\Delta R_{m,n}(\alpha^x)$.

In Table I we include the hardware results of the best architectures for NB-LDPC decoding and the results of our layered T-MM decoder with CNBMP. The code under test is for all the decoders the $(N=837,K=726)$ NB-LDPC code over $GF(32)$, with $d_c = 27$ and $d_v = 4$ [13]. Cadence RTL Compiler was used for the synthesis and SOC encounter for place and route of the design employing a 90nm CMOS process of nine layers with standard cells and operating conditions of $25^\circ C$ and 1.2V. Compared with a conventional implementation of T-MM algorithm, CNBMP decoder improves the requirements of area due to the reduction of storage resources in the check-node, in a layered schedule. On the other hand, the clock frequency is increased owing to the reduction of the wiring congestion and the core area in general. Additionally, we eliminate some pipeline stages in the decoder thanks to the reduction in the complexity of the check-node processor and hence the critical path is also reduced. These facts contribute to increment the overall throughput of the decoder.

If we compare this work to the most efficient architectures found in literature [7] and [8], we can see that the maximum frequency is increased in 50% and 26% respectively due to the reduction of the routing congestion. On the other hand, area is about 43% larger than the decoder from [7] and 3 times smaller than the one in [8]. After applying the CNBMP the area of storage resources (RAM memories and registers) is reduce from 80% ($2.2 \times 10^6$ NAND gates) of the total area in [8] to 50% ($0.62 \times 10^6$ NAND gates). About the throughput, the CNBMP proposal is 1.48 times faster than the T-MM decoder in [8] and 14.8 times faster than the Min-max from [7]. In terms of efficiency Throughput/Area the decoder with CNBMP is 3.9 times more efficient than [7] and [8]. For the gate count, we consider the equivalence of one bit of RAM equals to 1.5 NAND gates and one register equals to 4.5 NAND gates.

Finally, if we compare CNBMP to the binary LDPC decoder from [9], which has a gate count of 3.4 millions of equivalent NAND gates and a throughput of 45.42Gbps for a code with a similar rate and half codeword length in terms of bits ((2048, 1723) LDPC code), CNBMP has 2.72 times less gates and reaches 17.46 times less throughput$^1$. So, in terms of Throughput/Area efficiency, our non-binary decoder is 6.32 times less efficient than the binary one. Even not reaching the efficiency of a binary decoder, with CNBMP we reduce the difference to less than $q$, which is a good step forward compared to solutions like the one in [8] that has $2 \times q$ times lower efficiency.
V. CONCLUSIONS

In this paper a new message-passing definition is proposed for NB-LDPC decoders. This method reduces the number of the messages exchanged between check node and variable node, simplifying the routing of the derived hardware architectures and saving a big percentage of storage resources. Moreover, the new message passing does not modify the processing of the information at the decoder, keeping the same error correction performance as the original message-passing.

VI. ACKNOWLEDGEMENT

This research was supported by the Spanish Ministerio de Ciencia e Innovación, under Grant No. TEC2011-27916.

F. García-Herrero has a FPU grant sponsored by the Spanish Ministerio de Educación (Grant No. AP2010-5178).

REFERENCES

