Pseudocodewords from Bethe Permanents

Roxana Smarandache*
Departments of Mathematics and Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556 USA
rsmarand@nd.edu

***Abstract*—It was recently conjectured that a vector with components equal to the Bethe permanent of certain submatrices of a parity-check matrix is a pseudocodeword. In this paper, we analyze some important cases for which the conjecture is true and investigate the obtained families of pseudocodewords.**

***Index Terms*—Bethe-permanents, permanents, pseudocodewords.**

I. INTRODUCTION

In [1], a simple technique is presented for upper bounding the minimum Hamming distance of a binary linear code that is described by an $m \times n$ parity-check matrix $\mathbf{H}$. This is done based on explicitly constructing codewords with components equal to $\mathbb{F}_2$-determinants of some $m \times m$ submatrices of $\mathbf{H}$. Subsequently, this technique was extended and refined in [2]–[8] in the case of quasi-cyclic binary linear codes. By computing those determinant components over the ring of integers $\mathbb{Z}$ instead of over the binary field $\mathbb{F}_2$ (and taking their absolute value) it was shown that the resulting integer vectors are pseudocodewords, called *absdet-pseudocodewords*, i.e., vectors that lie in the fundamental cone of the parity-check matrix of the code [9], [10]. In addition, in [4], a closely related class of pseudocodewords called *perm-pseudocodewords* was defined, obtained by taking the vector components to be equal to the $\mathbb{Z}$-permanent of some $m \times m$ submatrices of $\mathbf{H}$.'

Related to the construction of perm-pseudocodewords, Vontobel introduced in [11, Sec. IX] a similar vector but having components equal to the Bethe permanent of some $m \times m$ submatrices of a matrix $\mathbf{H}$ instead of the regular permanent, and conjectured that this vector is a pseudocodeword. The term *Bethe permanent* was first used by Vontobel in [11], while the concept was introduced earlier in [12], [13], to denote the approximation of a permanent of a non-negative matrix, i.e., of a matrix containing only non-negative real entries, by solving a certain Bethe free energy minimization problem. In his paper [11], Vontobel provided some reasons why the approximation works well, by showing that the Bethe free energy is a convex function and that the sum-product algorithm finds its minimum efficiently. Therefore, the Bethe permanent can be computed efficiently (i.e., in polynomial time) and so can be the Bethe perm-pseudocodeword based on a set $\mathcal{S}$ of some given column selection of the parity-check matrix. This is not the case for the perm-pseudocodeword. Therefore, the set of Bethe perm-pseudocodewords, together with that of absdet-pseudocodewords, also efficiently computed due to the polynomial-time computation of the determinant, constitute useful objects in determining upper bounds on the minimum pseudo-weight and guiding the design of low-density parity-check matrices. In this paper we give four equivalent statements of the conjecture and discuss a stronger version of the above mentioned conjecture in some cases.

The remainder of the paper is structured as follows. In Section II, we list basic notations and definitions, provide the necessary background, formally define the class of perm-pseudocodewords and Bethe permanent vectors and state the conjecture. In Section III, we give a few examples to better illustrate the new notions and the conjecture. In Section IV, we show how the conjecture can be simplified to include only matrices of a certain form for which only one inequality is needed and from this, how the conjecture is equivalent to a certain co(perm)factor expansion on a row of a square matrix. We discuss the rows of the parity-check matrix of degree 2 or lower in Section V-A, prove a stronger version of the conjecture for two special cases in Sections V-B and V-C and discuss the next case of interest in Section V-D.

II. DEFINITIONS, VONTOBEL'S CONJECTURE AND EXAMPLES

Let $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{F}_2$ be the ring of integers, the field of real numbers, and the finite field of size 2, respectively. If $\mathbf{H}$ is some matrix and if $\alpha = \{i_1, \ldots, i_r\}$ and $\beta = \{j_1, \ldots, j_s\}$ are subsets of the row and column index sets, respectively, then $\mathbf{H}_{\alpha,\beta}$ is the sub-matrix of $\mathbf{H}$ that contains only the rows of $\mathbf{H}$ whose index appears in the set α and only the columns of $\mathbf{H}$ whose index appears in the set β. If α is the set of all row indices of $\mathbf{H}$, we will simply write $\mathbf{H}_\beta$ instead of $\mathbf{H}_{\alpha,\beta}$. Moreover, for any set of indices γ, we will use the short-hand $\gamma \setminus i$ for $\gamma \setminus \{i\}$. For an integer M, we will use the common notation $[M] \triangleq \{1, \ldots, M\}$. For a set α, $|\alpha|$ will denote the cardinality of α (the number of elements in the set α). The set of all $M \times M$ permutation matrices will be denoted by $\mathcal{P}_M$. The set of all permutations on the set $[m]$ is denoted by $\mathcal{S}_m$.

Definition 1. *Let $\theta = (\theta_{ij})$ be an $m \times m$-matrix over some commutative ring. Its determinant and permanent, respectively, are defined to be*

* Supported by NSF Grant CCF-1252788.

$$\det(\theta) \triangleq \sum_{\sigma\in\mathcal{S}_m} \mathrm{sgn}(\sigma) \prod_{i\in[m]} \theta_{i\sigma(i)}\ , \ \mathrm{perm}(\theta) \triangleq \sum_{\sigma\in\mathcal{S}_m} \prod_{i\in[m]} \theta_{i\sigma(i)}\ ,$$

where $\mathrm{sgn}(\sigma)$ *is the signature operator.* □

In this paper, we consider only permanents over the integers.

Definition 2. *Let* $\mathbf{H} = (h_{ij})$ *be an* $m \times n$ *parity-check matrix of some binary linear code. The fundamental cone* $\mathcal{K}(\mathbf{H})$ *of* $\mathbf{H}$ *is the set of all vectors* $\boldsymbol{\omega} = (\omega_i) \in \mathbb{R}^n$ *that satisfy*

$$\omega_j \geqslant 0 \qquad \text{for all } j \in [n] \tag{1}$$

$$\omega_j \leqslant \sum_{j'\in\mathrm{supp}(\mathbf{R}_i)\setminus j} \omega_{j'} \ \text{for all } i \in [m] \ \text{ and } j \in \mathrm{supp}(\mathbf{R}_i) \tag{2}$$

where $\mathbf{R}_i$ *is the ith row vector of* $\mathbf{H}$ *and* $\mathrm{supp}(\mathbf{R}_i)$ *is its support. A vector* $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$ *is called a* pseudocodeword *[14]. Two pseudocodewords* $\boldsymbol{\omega}, \boldsymbol{\omega}' \in \mathcal{K}(\mathbf{H})$ *are said to be in the same equivalence class if there exists an* $\alpha > 0$ *such that* $\boldsymbol{\omega} = \alpha \cdot \boldsymbol{\omega}'$. *In this case, we write* $\boldsymbol{\omega} \propto \boldsymbol{\omega}'$. □

Definition 3. *Let* $\mathcal{C}$ *be a binary linear code described by a parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m < n$. *For a size-*$(m{+}1)$ *subset* β *of* $[n]$ *we define the perm-vector based on* β *to be the vector* $\boldsymbol{\omega} \in \mathbb{Z}^n$ *with components*

$$\omega_i \triangleq \begin{cases} \mathrm{perm}\left(\mathbf{H}_{\beta\setminus i}\right) & \text{if } i \in \beta \\ 0 & \text{otherwise .} \end{cases}$$ □

The permanent operator is taken over $\mathbb{Z}$. In [4] it was shown that these vectors are in fact pseudocodewords. We state this here for easy reference together with its proof.

Theorem 4. *(from [4]) Let* $\mathcal{C}$ *be a binary linear code described by the parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m < n$, *and let* β *be a size-*$(m{+}1)$ *subset of* $[n]$. *The perm-vector* $\boldsymbol{\omega}$ *based on* β *is a pseudocodeword of* $\mathbf{H}$.

Example 5. Consider the $[4, 2, 2]$ binary linear code $\mathcal{C}$ based on the parity-check matrix $\mathbf{H} \triangleq \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$, where $n = 4$ and $m = 2$. The following list contains the perm-vectors based on all possible subsets $\beta \subset [4]$ of size $m{+}1 = 3$: $(2, 1, 1, 0)$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 1, 1, 2)$. It can be easily checked that these satisfy the inequalities of the fundamental cone above, as the theorem predicts. They give an upper bound on the minimum pseudo-weight of $8/3$.[1] □

The following combinatorial description of the Bethe permanent can be found in [11]. We use it here as a definition.

Definition 6. *Let* θ *be a non-negative (with non-negative real entries)* $m \times m$ *matrix and* M *be a positive integer. Define*

$$\Psi_{m,n,M} \triangleq \mathcal{P}_M^{m\times n} = \{\mathbf{P} = (P_{ij})_{\substack{i\,\in\,[m] \\ j\,\in\,[n]}} \mid P_{ij} \in \mathcal{P}_M\}.$$

If $m = n$, *we will use* $\Psi_{m,M} \triangleq \Psi_{m,n,M}$.

[1]The binary-input AWGNC pseudo-weight of a pseudocodeword $\boldsymbol{\omega} \neq \mathbf{0}$ is defined as [14]–[17] $w_{\mathrm{P}}^{\mathrm{AWGNC}}(\boldsymbol{\omega}) \triangleq \frac{\|\boldsymbol{\omega}\|_{\ell^1}^2}{\|\boldsymbol{\omega}\|_{\ell^2}^2}$, where $\|\cdot\|_{\ell^1}$ and $\|\cdot\|_{\ell^2}$ are, respectively, the 1-norm and 2-norm.

For a matrix $\mathbf{P} \in \Psi_{m,M}$, *the* $\mathbf{P}$*-lifting of* θ *is defined as the* $mM \times mM$ *matrix*

$$\theta^{\uparrow\mathbf{P}} \triangleq \begin{pmatrix} \theta_{11}P_{11} & \ldots & \theta_{1m}P_{1m} \\ \vdots & & \vdots \\ \theta_{m1}P_{m1} & \ldots & \theta_{mm}P_{mm} \end{pmatrix},$$

and the degree-M *Bethe permanent of* θ *is defined as*

$$\mathrm{perm}_{\mathrm{B},M}(\theta) \triangleq \sqrt[M]{\left\langle \mathrm{perm}(\theta^{\uparrow\mathbf{P}}) \right\rangle_{\mathbf{P}\in\Psi_{m,M}}},$$

where the angular brackets represent the arithmetic average of $\mathrm{perm}(\theta^{\uparrow\mathbf{P}})$ *over all* $\mathbf{P} \in \Psi_{m,M}$.

Then, the Bethe permanent of θ *is defined as*

$$\mathrm{perm}_{\mathrm{B}}(\theta) \triangleq \limsup_{M\to\infty} \mathrm{perm}_{\mathrm{B},M}(\theta).$$ □

Remark 7. Note that a $\mathbf{P}$-lifting of a matrix θ corresponds to an M-graph cover of the protograph (base graph) described by θ. Therefore we can consider $\theta^{\uparrow\mathbf{P}}$ to represent a protograph-based LDPC code and θ to be its protomatrix (also called its base matrix or its mother matrix) [18]. □

Definition 8. *Let* $\mathcal{C}$ *be a binary linear code described by a parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m < n$. *For a size-*$(m{+}1)$ *subset* β *of* $[n]$ *we define the Bethe permanent vector based on* β *to be the vector* $\boldsymbol{\omega}_{\mathrm{B}} \in \mathbb{R}^n$ *with components*

$$\omega_{\mathrm{B},i} \triangleq \begin{cases} \mathrm{perm}_{\mathrm{B}}\left(\mathbf{H}_{\beta\setminus i}\right) & \text{if } i \in \beta \\ 0 & \text{otherwise .} \end{cases}$$

Similarly, we define degree-M *Bethe permanent vector based on* β *to be the vector* $\boldsymbol{\omega}_{\mathrm{B},M} \in \mathbb{R}^n$ *with components*

$$\omega_{\mathrm{B},M,i} \triangleq \begin{cases} \mathrm{perm}_{\mathrm{B},M}\left(\mathbf{H}_{\beta\setminus i}\right) & \text{if } i \in \beta \\ 0 & \text{otherwise .} \end{cases}$$ □

The following conjecture is stated in [11].

Conjecture 9 ([11])**.** *Let* $\mathcal{C}$ *be a binary linear code described by an* $m \times n$ *binary parity-check matrix* $\mathbf{H}$, *with* $m < n$, *and let* β *be a size-*$(m + 1)$ *subset of* $[n]$. *Then the Bethe permanent vector* $\boldsymbol{\omega}_{\mathrm{B}}$ *based on* β *is a pseudocodeword of* $\mathbf{H}$, *i.e.,* $\boldsymbol{\omega}_{\mathrm{B}} \in \mathcal{K}(\mathbf{H})$.

III. Examples

In this section we provide several examples in order to get a better feeling of what perm- and Bethe permanent pseudocodewords look like.

Example 10. Consider the $[4, 2, 2]$ binary linear code $\mathcal{C}$ described in Example 5. The following list contains the degree-M Bethe permanent vectors based on all possible subsets $\beta \subset [4]$ of size $m{+}1 = 3$: $((M + 1)^{1/M}, 1, 1, 0))$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 1, 1, (M{+}1)^{1/M})$. It can be easily checked that all the above vectors satisfy the inequalities of the fundamental cone above, so they are all pseudocodewords. They give an upper bound on the minimum pseudo-weight of $8/3$, obtained for $M = 1$ case in which the set of perm-pseudocodewords listed in Example 5 is equal to the set of the degree-M Bethe permanent vectors described above. Taking the limit $M \to \infty$

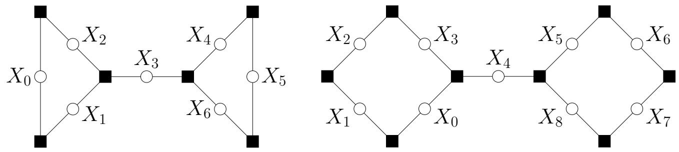

Fig. 1. Tanner graphs of dumbbell-graph-based codes. Left: $[7, 2, 3]$ binary linear code. Right: $[9, 2, 4]$ binary linear code.

we obtain the following list of Bethe permanent vectors based on all possible subsets $\beta \subset [4]$ of size $m+1 = 3$: $(1, 1, 1, 0)$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 1, 1, 1)$ all of pseudo-weight 3. □

Example 11. Let $M = 3$, P^s, $s = 0, 1, 2$, be the s-times cyclically left-shifted identity matrices of size $M \times M$ and $\mathbf{H} = \begin{bmatrix} I & I & I & I \\ 0 & I & P & P^2 \\ 0 & I & P^2 & P \end{bmatrix}$. We computed some of the Bethe permanent vectors of length12 and their pseudo-weights based on five column sets of length $3M + 1 = 10$ and included them in Table I, together with the perm-vectors based on the same sets of columns and their pseudo-weight for comparison. Since the sizes of the matrices are small in this example, their permanents can be easily computed. If the matrices are large, the perm-vectors can not be computed anymore and the approximation given by the Bethe permanents will be valuable. Even for relative small matrices (of size 100), computing the permanent is not immediate, while estimating the Bethe permanent is. □

Example 12. Consider the dumbbell-graph-based $[7, 2, 3]$ binary linear code described by the Tanner graph in Figure 1 (left). There is only one subset β of size $m+1 = 7$. It yields one perm-pseudo-codeword $(2, 2, 2, 4, 2, 2, 2)$ of pseudo-weight 6.4 and a Bethe permanent pseudocodeword $(1, 1, 1, 1, 1, 1, 1)$ of pseudo-weight 7. □

Example 13. Consider the dumbbell-graph-based $[9, 2, 4]$ binary linear code described by the Tanner graph in Figure 1 (right). It yields the perm-pseudo-codewords $(2, 2, 2, 2, 4, 2, 2, 2, 2)$ of pseudo-weight 8.3333 and the Bethe -permanent $(1, 1, 1, 1, 1, 1, 1, 1, 1)$ of pseudo-weight 9. □

Remark 14. Despite the fact that the permanent is lower bounded by the Bethe permanent [19], $\mathrm{perm_B}(\theta) \leqslant \mathrm{perm}(\theta)$, we observe that in all our examples, the pseudo-weights of the perm-vectors are lower than the pseudo-weights of the Bethe-permanent vectors. In general, however, there is no immediate reason why this should happen. □

Remark 15. The examples provided are for small size matrices, for which the permanent can be easily computed. The Bethe permanent better shows its usefulness in cases for which computing the permanent is too complex and the Bethe permanent is used as a close approximation and a close upper bound on the pseudo-weight. For example, matlab computes in a second the Bethe permanent of the 73×73 parity-check matrix of the code based on the projective geometry PG$(2, 8)$, but gets stuck when computing its permanent.[2] □

IV. An Equivalent Form of the Conjecture

In the following we show that it is enough to prove Vontobel's conjecture for a matrix having a column of weight 1. From this, we will show another equivalent description involving only square matrices. The Bethe-perm vectors are based on a set β of size $m + 1$, therefore, we can assume, without loss of generality, that $n = m + 1$. All the proofs in this and the remaining sections will be omitted; we invite the reader to see [22] for the complete proofs.

Theorem 16. *The following statements are equivalent.*
1) The conjecture holds for all $m \times (m + 1)$ matrices $\mathbf{H}$.
2) The conjecture holds for all $m \times (m + 1)$ matrices $\mathbf{H}$ with a column of Hamming weight 1.
3) For any $m \times (m + 1)$ binary matrix $\mathbf{H}$ with the first column equal to $[1\ 0\ \cdots\ 0]^\mathsf{T}$, the following inequality holds

$$\boldsymbol{\omega}_{\mathrm{B},1} \leqslant \sum_{l \in \mathrm{supp}(\mathbf{R}_1) \setminus 1} \boldsymbol{\omega}_{\mathrm{B},l}. \tag{3}$$

4) For any $m \times m$ binary (square) matrix $\mathbf{T} = (t_{ij})_{1 \leqslant i,j \leqslant m}$, its Bethe permanent is less than or equal to its "permanent-co(perm)factor expansion" along any one of its rows,[3] i.e.,

$$\mathrm{perm_B}\left(\mathbf{T}\right) \leqslant \sum_{l \in [m]} t_{il} \cdot \mathrm{perm_B}\left(\mathbf{T}_{[m]\setminus i, [m]\setminus l}\right), \ \forall i \in [m]. \tag{4}$$

Remark 17. Therefore, in order to prove the conjecture, we can assume that $\mathbf{H}$ has its first column equal to $[1\ 0\ \cdots\ 0]^\mathsf{T}$ and prove that: $\boldsymbol{\omega}_{\mathrm{B},1} \leqslant \sum_{l \in \mathrm{supp}(\mathbf{R}_1) \setminus 1} \boldsymbol{\omega}_{\mathrm{B},l}$. Note that, in this case, $\boldsymbol{\omega}_{\mathrm{B},1} \geqslant \boldsymbol{\omega}_{\mathrm{B},l}$ for all $l \in \mathrm{supp}(\mathbf{R}_1) \setminus 1$, so the first component is the largest among the components indexed by the $\mathrm{supp}(\mathbf{R}_1)$. □

In addition, in most our considerations, we will show that $\boldsymbol{\omega}_{\mathrm{B},M}$ is a pseudocodeword, for all $M \geqslant 1$. Then, by taking the limit it will follow that $\boldsymbol{\omega}_{\mathrm{B}} \in \mathcal{K}(\mathbf{H})$.

Lemma 18. *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$, and β be a size-$(m+1)$ subset β of $[n]$. Let $\boldsymbol{\omega}_{\mathrm{B},M}$ and $\boldsymbol{\omega}_{\mathrm{B}}$ based on β defined as in Definition 8. If $\boldsymbol{\omega}_{\mathrm{B},M} \in \mathcal{K}(\mathbf{H})$, for all integers $M \geqslant 1$, then $\boldsymbol{\omega}_{\mathrm{B}} \in \mathcal{K}(\mathbf{H})$.*

V. Cases for which the Conjecture is True

A. Case of Row Degrees $\leqslant 2$.

If a row in the matrix $\mathbf{H}$ has weight 2 or lower, then the associated inequalities (2) are always satisfied. It follows that,

[2]Note that the Ryser's algorithm [20], one of the most efficient algorithms for computing the permanent, requires $\Theta(n \cdot 2^n)$ arithmetic operations [21].This is better than brute force but still exponential in the matrix size, while the number of real additions and multiplications needed to compute the determinant is in $O(n^3)$.

[3]By "permanent-co(perm)factor expansion" we mean that the terms in the expansion sums are all taken with the positive sign and the Bethe permanent replaces the determinant in the definition of the cofactor.

1.3702	1.3875	1.6875	1	1	1	1	1	1	1	0	0	8.8700
3	2	2	1	1	1	1	1	1	1	0	0	8.1667
1.6875	2.3704	1.6875	1	1	1	1	1	1	0	1	0	8.8870
2	3	2	1	1	1	1	1	1	0	1	0	8.1667
1.6875	1.6875	2.3704	1	1	1	1	1	1	0	0	1	8.8870
2	2	3	1	1	1	1	1	1	0	0	1	8.1667
1.6875	1.6875	1.6875	0	1	1	1	1	0	1	0	1	8.4150
2	2	2	0	1	1	1	1	0	1	0	1	8.0000
1.6875	1.6875	1.6875	1	0	1	1	1	0	0	1	1	8.4150
2	2	2	1	0	1	1	1	0	0	1	1	8.0000

TABLE I

PAIRS OF BETHE PERMANENT VECTORS AND PERM-VECTORS BASED ON FIVE SETS β, TOGETHER WITH THEIR RESPECTIVE AWGNC PSEUDO-WEIGHTS.

if the matrix has all rows of degree $\leqslant 2$, the Bethe permanent vector is a pseudocodeword.

Lemma 19. *Let $\mathbf{H}$ be an $m \times (m+1)$ binary matrix that has all its rows of degree 2 or lower. Then the Bethe permanent vector $\boldsymbol{\omega}_{\mathrm{B}}$ is a pseudocodeword.*

B. Case of $\mathbf{H}$ of the Form (5) *or, equivalently,* (6).

In Examples 10 and 11, we observed that the sets of the degree-M Bethe permanent vectors and the Bethe permanent vectors based on all possible subsets β form two sets of pseudocodewords. In this section, we show that this stronger version of the conjecture is always true for a more general case, that of

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ * & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ * & 1 & 1 & \cdots & 1 \end{pmatrix} \in \mathbb{F}_2^{m \times (m+1)}, \tag{5}$$

where $m \geqslant 2$ is an integer, and $*$ can be either 0 or 1. Using a similar reasoning as in Section IV, we can see that, in fact, it is enough to show the conjecture for a matrix $\mathbf{H}$ of the form

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & \cdots & 1 \end{pmatrix} \in \mathbb{F}_2^{m \times (m+1)}, \tag{6}$$

for which it is enough to show $\boldsymbol{\omega}_{\mathrm{B},1} \leqslant \sum_{l \in [m+1] \setminus 1} \boldsymbol{\omega}_{\mathrm{B},l}$, as in (3). This inequality can be rewritten as

$$\boxed{q_{m,M} \leqslant m^M \cdot q_{m-1,M},}$$

where

$$q_{m,M} \triangleq \frac{\displaystyle\sum_{P \in \Psi_{m-1,M}} \operatorname{perm} \begin{bmatrix} I & I & \cdots & I \\ I & P_{11} & \cdots & P_{1,m-1} \\ \vdots & \vdots & & \vdots \\ I & P_{m-1,1} & \cdots & P_{m-1,m-1} \end{bmatrix}}{(M!)^{(m-1)^2}},$$

and I is the identity matrix of size $M \times M$.

Note that, for the matrix in (6), $\boldsymbol{\omega}_{\mathrm{B},M}$ is equal to

$$\boldsymbol{\omega}_{\mathrm{B},M} = \left(q_{m,M}^{1/M}, q_{m-1,M}^{1/M}, \cdots, q_{m-1,M}^{1/M}, q_{m-1,M}^{1/M}, q_{m-1,M}^{1/M} \right).$$

The proof of the inequality requires some heavy manipulations; [22] contains the details. We state here the result.

Theorem 20. *Let $\mathbf{H}$ be of the form* (6)*. Then, for all $M \geqslant 1$, its degree-M Bethe permanent vectors $\boldsymbol{\omega}_{\mathrm{B},M}$ and its Bethe permanent vector $\boldsymbol{\omega}_{\mathrm{B}}$ based on $\beta \triangleq [m+1]$ are pseudocodewords. We call them* degree-M Bethe permanent pseudocodeword based on β *and the* Bethe permanent pseudocodeword based on β*, respectively.*

C. Case of $\mathbf{H}$ of the Form (7).

In this section, we show the conjecture for a matrix in a slightly more general form : we will assume that the first row of $\mathbf{H}$ contains less than $m+1$ ones, where $m \geqslant 2$ is an integer and $*$ can be either 0 or 1. We assume that $\operatorname{supp}(\mathbf{R}_1) < m+1$, and for simplicity, we will assume only one extra zero on the first row. Using a similar reasoning as in Section IV, we can see that, in fact, it is then enough to show the conjecture for a matrix $\mathbf{H}$ of the form

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{m \times (m+1)}, \tag{7}$$

for which, it is enough to show the inequality (3). This turns out to be equivalent to the following formal inequality:

$$\boxed{t_{m,M} \leqslant (m-1)^M \cdot q_{m-1,M},}$$

where

$$t_{m,M} \triangleq \frac{\displaystyle\sum_{Q \in \Psi_{m-1,M}} \operatorname{perm} \begin{bmatrix} I & \cdots & I & 0 \\ Q_{11} & \cdots & Q_{1,m-1} & I \\ \vdots & & \vdots & \vdots \\ Q_{m-1,1} & \cdots & Q_{m-1,m-1} & I \end{bmatrix}}{(M!)^{(m-1)^2}}.$$

Note that for the matrix in (7), $\boldsymbol{\omega}_{\mathrm{B},M}$ is equal to

$$\boldsymbol{\omega}_{\mathrm{B},M} = \left(t_{m,M}^{1/M}, q_{m-1,M}^{1/M}, q_{m-1,M}^{1/M}, \cdots, q_{m-1,M}^{1/M} \right).$$

Therefore, by adding one zero to the all-one matrix $\theta = \mathbf{H}_{[m+1] \setminus 1}$, with $\mathbf{H}$ given in (6), we decrease the upper bound on its degree-M Bethe permanent from $m \cdot q_{m-1,M}^{1/M}$ (see (V-B)) to $(m-1)\cdot q_{m-1,M}^{1/M}$ for the submatrix of the matrix in (7) with columns indexed by the same set $[m+1]\setminus 1$. Similarly, when we further increase the number of zeros on the first row of the all-one matrix, we further decrease the upper bound on its degree-M Bethe permanent from $m\cdot q_{m-1,M}^{1/M}$ to $(\mathrm{supp}(\mathbf{R}_1)-1)\cdot q_{m-1,M}^{1/M}$. Therefore, any extra zero on one row of the all-one matrix, produces a decrease in the upper bound of its degree-M Bethe permanent by one quantity $q_{m-1,M}^{1/M}$.

Theorem 21. *Let $\mathbf{H}$ be of the form in* (7). *Then, for all $M \geqslant 1$, its degree-M Bethe permanent vectors $\boldsymbol{\omega}_{\mathrm{B},M}$ and its Bethe permanent vector $\boldsymbol{\omega}_{\mathrm{B}}$ based on $\beta \triangleq [m+1]$ are pseudocodewords for $\mathbf{H}$.*

D. Case of $\mathbf{H}$ of the Form (8).

The natural next step to consider is that of a matrix $\mathbf{H}$ with allowed zeros in the first two rows and ones elsewhere. We will consider the simplest case and discuss the problems that this case presents. Let

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{m\times(m+1)} \tag{8}$$

and

$$\boxed{\hat{t}_{m,M}^{1/M} \leqslant (m-1)\cdot t_{m-1,M}^{1/M} + q_{m-1,M}^{1/M},}$$

where

$$\hat{t}_{m,M} \triangleq \frac{\sum\limits_{Q\in\Psi_{m-1,M}} \mathrm{perm}\begin{bmatrix} I & \cdots & I & 0 \\ Q_{11} & \cdots & 0 & I \\ \vdots & & \vdots & \vdots \\ Q_{m-1,1} & \cdots & Q_{m-1,m-1} & I \end{bmatrix}}{(M!)^{(m-1)^2-1}}.$$

Note that for the matrix in (7), $\boldsymbol{\omega}_{\mathrm{B},M}$ is equal to

$$\boldsymbol{\omega}_{\mathrm{B},M} = \left(\hat{t}_{m,M}^{1/M}, t_{m-1,M}^{1/M}, \cdots, t_{m-1,M}^{1/M}, q_{m-1,M}^{1/M}, t_{m-1,M}^{1/M}\right).$$

The difficulty of this case lies in the fact that on the right hand side of the inequality $\hat{t}_{m,M}^{1/M} \leqslant (m-1)\cdot t_{m-1,M}^{1/M} + q_{m-1,M}^{1/M}$, there are Mth roots of non-equal terms. We show this on the simple case of $m=3$, for which the inequality becomes: $\hat{t}_{3,M}^{1/M} \leqslant 1 + (M+1)^{1/M}$, since the vector $\boldsymbol{\omega}_{\mathrm{B},M}$ is equal to

$$\boldsymbol{\omega}_{\mathrm{B},M} = \left(\hat{t}_{3,M}^{1/M}, 1, q_{2,M}, 1\right) = \left(\hat{t}_{3,M}^{1/M}, 1, (M+1)^{1/M}, 1\right).$$

We solved this particular case by computing an exact formula for $\hat{t}_{3,M}^{1/M}$, $\hat{t}_{3,M} = \frac{\sum_{r=0}^{M}\binom{M}{r}\sum_{s=0}^{r}\binom{r}{s}(M-r+s)!(M-s)!r!}{M!^2}$, and plotting $\hat{t}_{3,M}^{1/M}$ and $1+(M+1)^{1/M}$, to see that $\hat{t}_{3,M}^{1/M} \leqslant 1+(M+1)^{1/M}$ [22]. The case of $m \geqslant 4$ remains open for the most general setting. For matrices with a lot of zeros, it might be possible to compute the degree-M Bethe permanents exactly (as in the case $m=3$), using combinatorial arguments, by showing, for example, that the permanents of a block $mM\times mM$ matrix is equal to the permanent of a smaller matrix. In [22], we illustrate this idea with an example.

Acknowledgements

We thank Pascal O. Vontobel and Martin Haenggi for the many discussions on this topic.

References

[1] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)* (B. Marcus and J. Rosenthal, eds.), vol. 123 of IMA Vol. Math. Appl., pp. 113–130, Springer Verlag, New York, Inc., 2001.

[2] R. Smarandache and P. O. Vontobel, "On regular quasi-cyclic LDPC codes from binomials," in *IEEE Intern. Symp. on Inform. Theory*, (Chicago, IL, USA), p. 274, June 27–July 2 2004.

[3] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. Inform. Theory*, vol. 58, pp. 585–607, Feb. 2012.

[4] R. Smarandache and P. O. Vontobel, "Absdet-pseudo-codewords and perm-pseudo-codewords: definitions and properties," in *IEEE Intern. Symp. on Inform. Theory*, (Seoul, Korea), June 2009.

[5] B. K. Butler and P. H. Siegel, "Bounds on the Minimum Distance of Punctured Quasi-Cyclic LDPC Codes," *ArXiv e-prints*, Jan. 2012.

[6] Y. Wang, S. C. Draper, and J. S. Yedidia, "Hierarchical and High-Girth QC LDPC Codes," *ArXiv e-prints*, Nov. 2011.

[7] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Design of Multiple-Edge Protographs for QC LDPC Codes Avoiding Short Inevitable Cycles," *ArXiv e-prints*, Oct. 2012.

[8] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Protograph design with multiple edges for regular QC LDPC codes having large girth," in *IEEE Intern. Symp. on Inform. Theory*, pp. 918 – 922, 2011.

[9] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 2003.

[10] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inform. Theory*, vol. 51, pp. 954–972, Mar. 2005.

[11] P. O. Vontobel, "The Bethe permanent of a non-negative matrix," *to appear in IEEE Trans. Inf. Theory*, 2013. Available online at http://arxiv.org/abs/1107.4196.

[12] B. Huang and T. Jebara, "Approximating the Permanent with Belief Propagation," *ArXiv e-prints*, Aug. 2009.

[13] M. Chertkov, L. Kroc, and M. Vergassola, "Belief Propagation and Beyond for Particle Tracking," *ArXiv e-prints*, June 2008.

[14] P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," *CoRR*, Dec. 2005. Available at http://www.arxiv.org/abs/cs.IT/0512078.

[15] N. Wiberg, *Codes and Decoding on General Graphs*. PhD thesis, Linköping University, Sweden, 1996.

[16] G. D. Forney, Jr., R. Koetter, F. R. Kschischang, and A. Reznik, "On the effective weights of pseudocodewords for codes defined on graphs with cycles," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)* (B. Marcus and J. Rosenthal, eds.), vol. 123 of *IMA Vol. Math. Appl.*, pp. 101–112, Springer Verlag, New York, Inc., 2001.

[17] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *3rd Intern. Symp. on Turbo Codes and Related Topics*, (Brest, France), pp. 75–82, Sept. 1–5 2003.

[18] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," *IPN Progress Report*, vol. 42-154, pp. 1–7, 2003.

[19] L. Gurvits, "Unleashing the power of Schrijver's permanental inequality with the help of the Bethe Approximation," *ArXiv e-prints*, June 2011.

[20] H. J. Ryser, "Combinatorial mathematics (Carus Mathematical Monographs No. 14)," *Mathematical Association of America*, 1963.

[21] L. Valiant, "The complexity of computing the permanent," *Theor. Comp. Sc.*, vol. 8, no. 2, pp. 189–201, 1979.

[22] R. Smarandache, "Pseudocodewords from Bethe permanents," *Submitted to IEEE Trans. Inf. Theory*, Nov. 2011. Available online at http://arxiv.org/abs/1112.4625.