On Phase Correct Blind Deconvolution of Flat MIMO Channels Exploiting Channel Encoding

Ansgar Scherb, Volker Kühn and Karl-Dirk Kammeyer
Department of Communications Engineering
University of Bremen
Otto-Hahn-Allee
D-28359 Bremen, Germany
Email:{scherb, kuehn, kammeyer}@ant.uni-bremen.de

***Abstract*— In this paper we propose a new algorithm separating blindly the sources of a flat MIMO-communication link, where all sources are independently channel encoded. To this end the proposed method exploits statistical dependencies caused by the channel code for blindly estimating the channel and simultaneously adjusting a linear equalizer. In contrast to most common blind source separation methods the suggested method completely resolves the phase and permutation ambiguity of the estimated channel impulse response and the equalizer. The performance of the presented method will be evaluated by numerical results.**

I. Introduction

Most blind source separation (BSS) methods as e.g. [1], [2], [3], [4] are based on the assumption of statistically independent and non gaussian distributed sources. The channel causes a linear superposition of these sources. As stated by the central limit theorem, the distribution of the channel output is more similar to the gaussian distribution than the channel input. Thus, the key idea behind blind source separation is to design blindly (without channel state information) a linear equalizer such that the equalizer restores the statistical independence. To this end the equalizer's output has to be uncorrelated and as less gaussian as possible.

Generally, the receiver does not need to know the exact probability density function of the sources in order to blindly separate them. However, in a MIMO-communication link the degree of knowledge at the receiver is much higher, since the source signals are usually defined on a finite alphabet such as PSK, QAM, etc. and the transmitted data are protected against errors by a channel code.

In this paper we will propose a method for BSS, which exploits statistical dependencies caused by channel coding in order to blindly identify the channel and simultaneously adjust a linear equalizer. In contrast to most common BSS methods the suggested method completely resolves the phase and permutation ambiguity of the estimated channel impulse response and the corresponding linear equalizer. In order to achieve this target the channel code has to satisfy an asymmetry condition. In [5], [6] asymmetric signaling constellations were utilized for phase correct blind estimation techniques. However, code asymmetry does not necessarily involve symbol asymmetry. A similar approach for blind deconvolution of frequency selective SISO channels was suggested in [7].

This paper is organized as follows: In Section II the system model will be presented. Since channel coding plays a key role for the proposed method, we will discus some required properties of channel codes and give some definitions in Section III. The presented algorithm will be derived in Section IV. Finally we give numerical results in Section V and conclude this paper in Section VI.

II. System Model

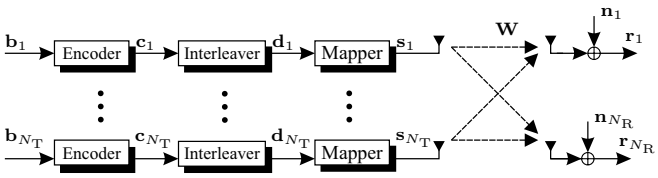

Fig. 1. System Model

As illustrated in Fig. 1, we consider a layered block transmission of N_T independent binary data streams $\mathbf{b}_m \in \{0,1\}^{(I\times 1)}$ of length I, where $m = 1, \cdots, N_\mathrm{T}$ is the layer index. After encoding each layer independently by a linear block encoder, we obtain

$$\mathbf{c}_m = \mathrm{mod}(\mathbf{G}\mathbf{b}_m, 2), \tag{1}$$

where $\mathbf{G} \in \{0,1\}^{(I\times K)}$ is the channel code generator matrix with rate $R_c = I/K < 1$ and $\mathbf{c}_m \in \{0,1\}^{K\times 1}$. Afterwards, at each layer the resulting bits are permuted by

$$\mathbf{d}_m = \mathbf{P}_m \mathbf{c}_m, \tag{2}$$

where the permutation matrix $\mathbf{P}_m \in \{0,1\}^{K\times K}$ is contains exactly one nonzero element in each row and column. Encoding und permutation can be summarized by the overall generator matrix $\tilde{\mathbf{G}}_m = \mathbf{P}_m\mathbf{G}$. Please note, that the generator matrix of a certain layer may coincide with any other, but the permutation matrix of each layer should differ, in order to make each layer distinguishable from any other.

After mapping the bits into the signal space by BPSK modulation assigning $0 \to 1$ and $1 \to -1$, the channel input is given by

$$\mathbf{s}_m = \mathrm{BPSK}(\mathbf{d}_m). \tag{3}$$

This data can be arranged in the matrix $\mathbf{S} = [\mathbf{s}_1, \cdots, \mathbf{s}_{N_\mathrm{T}}]^T = [\mathbf{s}(1), \cdots, \mathbf{s}(K)]$. The signal pass through a $(N_\mathrm{R} \times N_\mathrm{T})$ MIMO channel with $N_\mathrm{R} \geq N_\mathrm{T}$. Collecting N_R samples at instance k the channel output can be expressed as

$$\mathbf{r}(k) = \mathbf{W}\mathbf{s}(k) + \mathbf{n}(k) \tag{4}$$

where $\mathbf{W}$ is the MIMO channel impulse response (CIR) and $\mathbf{n}(k) \in \mathbb{C}^{N_\mathrm{R} \times 1}$ is i.i.d. white gaussian noise with covariance $\mathrm{E}\{\mathbf{n}(k)\mathbf{n}^H(k)\} = \sigma_n^2 \mathbf{I}_{N_\mathrm{R}}$.

III. Channel Coding

Since they are well suited for our purpose, throughout this paper we consider regular low density parity check (LDPC) codes for channel coding [8], [9]. A (K, I)-LDPC code is characterized by a sparse parity check matrix $\mathbf{H}$ of dimension $(L \times K)$, where the number of nonzero elements Ω in $\mathbf{H}$ is much lower than the number of zeros. The number of rows in $\mathbf{H}$ is at least $L \geq K - I$ and $\mathbf{H}$ has rank $K - I$. The relation

$$\mathrm{mod}(\mathbf{H}\mathbf{G}, 2) = \mathbf{0} \tag{5}$$

holds with respect to the corresponding generator matrix. Due to (5) the parity check sum equation

$$\mathrm{mod}(\mathbf{H}\mathbf{c}, 2) = \mathbf{0} \tag{6}$$

also holds for any encoded data bit stream $\mathbf{c} = \mathrm{mod}(\mathbf{G}\mathbf{b}, 2)$. Let $\mathbf{s} = \mathrm{BPSK}(\mathbf{c})$ be the BPSK signal space representation of $\mathbf{c}$ and $\mathcal{H}_l$ be the set of column indices according to the nonzero elements in the l-th row of $\mathbf{H}$. Then, analogue to (6) for $l = 1, \cdots, L$ the relation

$$\prod_{k \in \mathcal{H}_l} s(k) = 1 \tag{7}$$

holds. Let $\mathcal{C}$ be a set comprising of indices k corresponding to the null space of the code. Please note that in this case the expectation of the product with respect to $\mathcal{C}$ is

$$\mathrm{E}\Big\{ \prod_{k \in \mathcal{C}} s(k) \Big\} = 0. \tag{8}$$

A LDPC code is called regular, if the number of 1's in each row as well as the number of 1's in each column is exactly equal. Let κ denote the number of 1's in each row called right degree and λ the number of 1's in each column called left degree. Please note that the set $\mathcal{A}$ of all valid code words is uniquely defined by $\mathbf{H}$, whereas several generator matrices exist fulfilling (5).

Since we aim to obtain phase correct channel estimates, the signal space representation of any valid codeword should be unique independently from a complex factor. To this end the channel code should be asymmetric as stated in the following definition:

Definition 1: A channel code is called *asymmetric*, if the negation of an arbitrary valid code word is not a valid code word:

$$\mathbf{c} \in \mathcal{A} \Leftrightarrow \overline{\mathbf{c}} \notin \mathcal{A}$$

Obviously, a code is asymmetric if an arbitrary parity check sum includes an odd number of encoded bits. Thus, we can state following theorem:

Theorem 1: Let $\mathbf{H}$ be the parity check matrix of a linear channel code. If there exists a row or a linear combination of rows in $\mathbf{H}$ such that the number of 1's is odd, then this code is asymmetric.

Consequently, we restrict in the following to regular LDPC codes with odd κ.

Before starting with the derivation of the proposed algorithm, we prefix some reasonable set definitions.

Let $l(\tilde{l}, k)$ be the row of $\tilde{l}$-th nonzero element in the k-th column in $\mathbf{H}$ and define the circular weight of an element $x \in \mathcal{H}_{l(\tilde{l},k)}$ in the with respect the column index k as

$$W_{\text{circ}}(x, k) = \mathrm{mod}(x - k, K). \tag{9}$$

Then $\mathcal{H}_{\tilde{l},k}$ is defined as the set of the column indices according to all 1's in the l-th row sorted in ascending order with respect to their circular weights. Extracting k from $\mathcal{H}_{\tilde{l},k}$ the remaining elements can be separated into 2 equal sized subsets $\mathcal{H}_{l,k}^{(1|2)}$ comprising the first part and $\mathcal{H}_{l,k}^{(2|2)}$ comprising the second part.

Example: Let

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

be the (6×15) LDPC matrix. The second nonzero element of the seventh column is in row $l(2, 7) = 4$. The fourth row contains 1's in the columns 3, 7, 10 ,13, and 14 with circular weights $W_{\text{circ}}(3, 7) = 11$, $W_{\text{circ}}(7, 7) = 0$, $W_{\text{circ}}(10, 7) = 3$, $W_{\text{circ}}(13, 7) = 6$ and $W_{\text{circ}}(14, 7) = 7$, respectively. Thus, we obtain following sets: $\mathcal{H}_{2,7} = \{7, 10, 13, 14, 3\}$, $\mathcal{H}_{2,7}^{(1|2)} = \{10, 13\}$ and $\mathcal{H}_{2,7}^{(2|2)} = \{14, 3\}$.

In Tab. I all set definitions given in this section are summarized.

TABLE I
SET DEFINITIONS

$\mathcal{A}$	:	all valid code words
$\mathcal{H}_l$	:	all column indices according to the 1's in the l-th row of $\mathbf{H}$
$\mathcal{H}_{\tilde{l},k}$	:	all column indices according to the 1's in the $l(\tilde{l}, k)$-th row of $\mathbf{H}$ in ascending order w.r.t. their circular weights
$\mathcal{H}_{\tilde{l},k}^{(1\|2)}$	:	subset corresponding to the first part of $\mathcal{H}_{\tilde{l},k} \setminus \{k\}$
$\mathcal{H}_{\tilde{l},k}^{(2\|2)}$	:	subset corresponding to the second part of $\mathcal{H}_{\tilde{l},k} \setminus \{k\}$

IV. Proposed Algorithm

Let $\mathbf{e} \in \mathbb{C}^{N_\mathrm{R} \times 1}$ be a linear filter unequal zero,

$$y(k) = \mathbf{e}^H \mathbf{r}(k) \tag{10}$$

be the filter output at the receiver and $\mathbf{q} = \mathbf{W}^H \mathbf{e}$ be the overall impulse response of filter and channel. Furthermore, assume that $\mathbf{H}$ is the parity check matrix corresponding to the generator matrix $\tilde{\mathbf{G}}_m$ of the m-th layer. Selecting an arbitrary 1 in the parity check matrix $\mathbf{H}$, e.g. the $\tilde{l}$-th 1 in the k-th column, it can be shown that the m-th column $\mathbf{w}_m$ of the channel impulse response $\mathbf{W}$ weighted by some real positive factor is given by the expectation

$$\begin{aligned} &\mathrm{E}\Big\{\mathbf{r}(k) \prod_{\mu \in \mathcal{H}_{\tilde{l},k}^{(1|2)}} y(\mu) \prod_{\nu \in \mathcal{H}_{\tilde{l},k}^{(2|2)}} y^*(\nu)\Big\} \\ &= \mathrm{E}\Big\{\big(\mathbf{W}\mathbf{s}(k) + \mathbf{n}(k)\big) \\ &\quad \prod_{\mu \in \mathcal{H}_{\tilde{l},k}^{(1|2)}} \big(\mathbf{q}^H \mathbf{s}(\mu) + \eta(\mu)\big) \\ &\quad \prod_{\nu \in \mathcal{H}_{\tilde{l},k}^{(2|2)}} \big(\mathbf{s}^H(\nu)\mathbf{q} + \eta^*(\nu)\big)\Big\}, \end{aligned} \tag{11}$$

where $\eta(k) = \mathbf{e}^H \mathbf{n}(k)$.

Proof: Let k_ι be the ι-th member of $\mathcal{H}_{\tilde{l},k}$ and $\mathcal{M}$ be the set of κ-tuples with cardinality N_T^κ consisting of all combinations of layers indices. With these definitions expectation (11) can be rewritten as (12) in the bottom line of the next page. Since the noise is i.i.d, all elements incorporating noise vanish in (12). Assuming that no parity check sum is accidentally caught in $v(k_1, \cdots, k_\kappa, \tilde{m}_1, \cdots, \tilde{m}_\kappa)$, due to (8) this expression becomes zero and only the left term remains such that

$$\mathrm{E}\Big\{\mathbf{r}(k) \prod_{\mu \in \mathcal{H}_{\tilde{l},k}^{(1|2)}} y(\mu) \prod_{\nu \in \mathcal{H}_{\tilde{l},k}^{(2|2)}} y^*(\nu)\Big\} = \mathbf{w}_m |q_m|^{\kappa-1}. \tag{13}$$

Obviously, (13) is equivalent to the true channel coefficients $\mathbf{w}_m$ corresponding to the m-th layer, which is weighted by a real positive factor $|q_m|^{\kappa-1}$. This factor is real and positive, since phase rotation caused by the product according to the subset $\mathcal{H}_{\tilde{l},k}^{(1|2)}$ is compensated by the conjugated product according to the subset $\mathcal{H}_{\tilde{l},k}^{(2|2)}$. Recall that (13) holds for Ω different expectation arguments according to the 1's in $\mathbf{H}$. Thus, a phase correct channel estimator for $\mathbf{w}_m$ can be obtained by averaging over Ω different equations of this type, i.e.

$$\hat{\mathbf{w}}_m = \frac{1}{\Omega} \sum_{\tilde{l}=1}^{\lambda} \sum_{k=1}^{K} \mathbf{r}(k) \prod_{\mu \in \mathcal{H}_{\tilde{l},k}^{(1|2)}} y(\mu) \prod_{\nu \in \mathcal{H}_{\tilde{l},k}^{(2|2)}} y^*(\nu). \tag{14}$$

Since the estimation rule (14) approximates the expectation $v(k_1, \cdots, k_\kappa, \tilde{m}_1, \cdots, \tilde{m}_\kappa)$ in (12) by averaging, this term does not become exactly zero and an error remains weighted by $u(\kappa_1, \cdots, \kappa_M)$, whose power depends on the current filter adjustment. A readjustment of the filter $\mathbf{e}$ on the basis of the current channel estimate may assist reducing the impact of this error. If $\mathbf{e}$ is an ideal linear equalizer with respect to the m-th layer, the term $u(\kappa_1, \cdots, \kappa_M)$ weighting the remaining error becomes very small. Therefore, we suggest an iterative two-step algorithm, where channel estimation and filter adaptation are repeated alternately until the algorithm converges. Let i be an iteration counter, $\mathbf{e}_{(0)} = [1, \cdots, 1]^T$ be the initial equalizer at iteration $i = 0$, and $\mathbf{w}_m^{(i)}$ an channel estimate of the i-th step according to (14). On the basis of the channel estimate the filter's coefficients can be adjusted, e.g. by the MMSE approach with

$$\tilde{\mathbf{e}}_{(i+1)} = \mathbf{\Phi}_{rr}^{-1} \hat{\mathbf{w}}_m^{(i)}, \tag{15}$$

where $\mathbf{\Phi}_{rr} = \mathrm{E}\{\mathbf{r}(k)\mathbf{r}^H(k)\}$ is the covariance matrix of the receive signal. In order to avoid a bit overflow, $\tilde{\mathbf{e}}_{(i)}$ should be normalized by

$$\mathbf{e}_{(i)} = \frac{\tilde{\mathbf{e}}_{(i)}}{\sqrt{\tilde{\mathbf{e}}_{(i)}^H \mathbf{\Phi}_{rr} \tilde{\mathbf{e}}_{(i)}}}. \tag{16}$$

The algorithm is summarized in Tab. II.

TABLE II

Phase correct blind deconvolution exploiting channel coding (BDCC)

1	:	Initialize $\mathbf{e}_{(0)} = [1, \cdots, 1]^T$ and the iteration counter $i = 0$.
2	:	**repeat**
3	:	Estimate the channel by (14).
4	:	Update the linear equalizer by (15) and (16).
5	:	Set $i = i + 1$.
6	:	**end**

V. Numerical Results

In our simulation we used regular (λ, κ)-LDPC codes free of 4-cycles.

The signal was transmitted over an (4×4) block fading channel with i.i.d. zero mean complex gaussian distributed channel gains. As block length for one channel realization we considered $K = 100$, $K = 400$ or $K = 1600$. In order to achieve approximately the desired block length, the encoding was repeated several times and subsequently permuted by a random interleaver.

The estimation performance was evaluated by the normalized mean squared error (NMSE) between the true and the estimated channel:

$$\mathrm{NMSE} = \frac{\|\mathbf{w}_m - \hat{\mathbf{w}}_m\|^2}{\|\mathbf{w}_m\|^2} \tag{17}$$

The algorithms was stopped after 5 iterations. The results are averaged over 5000 channel realizations.

Fig. 2 and Fig. V shows the NMSE performance versus the E_b/N_0 ratio of the blind deconvolution exploiting channel coding (BDCC). All curves in 2 shows an error floor at high E_b/N_0 depending on the block length. However, the NMSE values are even considerable for block length $K = 100$. In

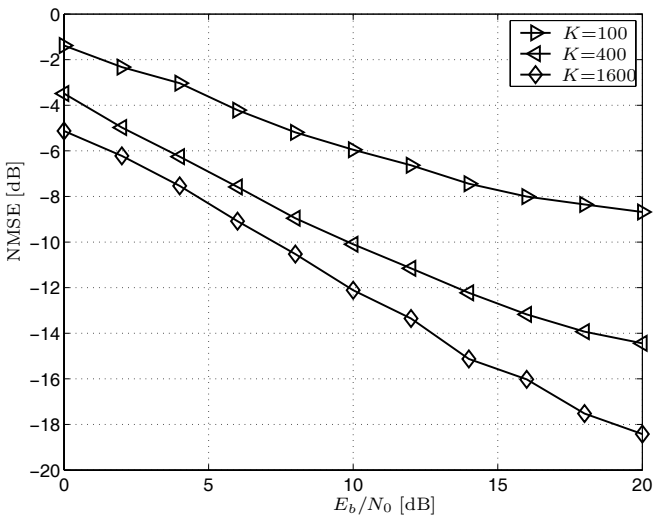

Fig. 2. NMSE vs. E_b/N_0 for channel code $(2,3)$-LDPC with block length $K = 100$, $K = 400$, $K = 1600$

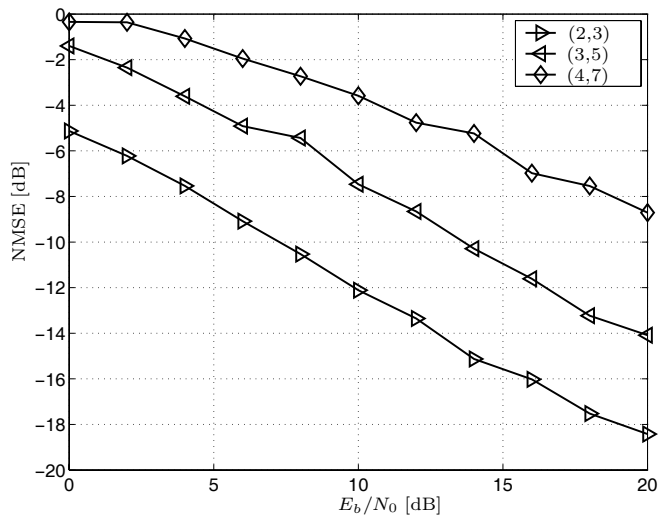

Fig. 3. NMSE vs. E_b/N_0 for channel code $(2,3) - LDPC$, $(3,5) - LDPC$ and $(4,7) - LDPC$ with block length $K = 1600$

Fig. V it can be observed, that the performance of the BDCC depends strongly on the right degree κ of the particular channel coding. The reason may be on the one hand that the number of terms, which are accumulated in (12), becomes very high for large κ and consequently the performance is very sensitive. On the other hand also the impact of noise on the estimation must be taken into account. For small κ the BDCC performs very well.

VI. Conclusions

In this paper we have derived an iterative algorithm, which blindly identifies a MIMO channel exploiting the statistical dependencies of the transmitted signal caused by channel coding. The algorithm jointly updates channel estimates and adapts a linear equalizer. For asymmetric channel coding, the algorithm delivers phase correct estimates. It was shown by simulations, that the performance of the proposed algorithm depends on code properties, i.e. the right degree of its parity check matrix. In the case of a short right degree the algorithm performs quite good.

References

[1] J.-F. Cardoso and A. Souloumiac. Blind beamforming for non gaussian signals. *IEE Proceedings-F*, 140(6):362370, 1993.

[2] M. Feng and K. D. Kammeyer. Blind Source Separation for Communication Signals Using Antenna Arrays. In *Proc. IEEE Int. Conference on Personal Wireless Communications (ICUPC-98)*, Florence, Italy, October 1998.

[3] A. Hyvarinen and E. Oja. Independent component analysis: algorithms and applications. *Neural Networks*, 13:411–430, May-June 2000.

[4] A. Bell and T. Sejnowski. An information-maximisation approach to blind separation and blind deconvolution.

[5] T. Thajupathump, C.D. Murphy, and S. A. Kassam. Assymemetric signaling constellation for phase estimation. In *The 10th IEEE Workshop on Statistical Signal and Array Processing*, Pocono, USA, August 2000.

[6] F. Sanzi and M. C. Necker. Totally blind APP channel estimation with higher order modulation schemes. *in Proc. IEEE Vehicular Tech. Conf. (VTCFall)*, October 2003.

[7] A. Scherb, V. Kuehn, and K. D. Kammeyer. On Phase Correct Blind Deconvolution exploiting Channel Coding. In *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 03)*, Darmstadt, Germany, December 2003.

[8] R. G. Gallager. *Low Density Parity Check Codes*. MIT Press, Cambridge, 1963.

[9] D. J. C. MacKay and R. M. Neal. Near Shannon limit performance of low density parity check. *Electron. Lett.*, 33(6):457–458, March 1997.

$$\mathbf{w}_m |q_m|^{\kappa-1} \underbrace{\mathrm{E}\Big\{ \prod_{k\in\mathcal{H}_{l,k}} s_m(k) \Big\}}_{=1} + \sum_{(\tilde{m}_1\cdots\tilde{m}_\kappa)\in\mathcal{M}\setminus(m\cdots m)} \underbrace{\mathbf{w}_{\tilde{m}_1} \prod_{\alpha=2}^{\kappa/2} q_{\tilde{m}_\alpha} \prod_{\beta=\kappa/2+1}^{\kappa} q^*_{\tilde{m}_\beta}}_{u(\tilde{m}_1,\cdots,\tilde{m}_\kappa)} \underbrace{\mathrm{E}\Big\{ \prod_{\gamma=1}^{\kappa} s_{\tilde{m}_\gamma}(k_\gamma) \Big\}}_{v(k_1,\cdots,k_\kappa,\tilde{m}_1,\cdots,\tilde{m}_\kappa)} \tag{12}$$