The Generalized Area Theorem and Some of its Consequences

Cyril Méasson,† Andrea Montanari,∗ Tom Richardson,+ and Rüdiger Urbanke‡

***Abstract*— There is a fundamental relationship between belief propagation and maximum a posteriori decoding. The case of transmission over the binary erasure channel was investigated in detail in a companion paper. This paper investigates the extension to general memoryless channels (paying special attention to the binary case). An area theorem for transmission over general memoryless channels is introduced and some of its many consequences are discussed. We show that this area theorem gives rise to an upper-bound on the maximum a posteriori threshold for sparse graph codes. In situations where this bound is tight, the extrinsic soft bit estimates delivered by the belief propagation decoder coincide with the correct a posteriori probabilities above the maximum a posteriori threshold. More generally, it is conjectured that the fundamental relationship between the maximum a posteriori and the belief propagation decoder which was observed for transmission over the binary erasure channel carries over to the general case. We finally demonstrate that in order for the design rate of an ensemble to approach the capacity under belief propagation decoding the component codes have to be perfectly matched, a statement which is well known for the special case of transmission over the binary erasure channel.**

***Index Terms*— belief propagation, maximum a posteriori, maximum likelihood, Maxwell construction, threshold, phase transition, Area Theorem, EXIT curve, entropy**

I. Introduction

It was shown in [3]–[5] that, when transmission takes place over the binary erasure channel (BEC) using sparse graph codes, there exists a surprising and fundamental relationship between the belief propagation (BP) and the maximum a posteriori (MAP) decoder. This relationship emerges in the limit of large blocklengths. Operationally, this relationship is furnished for the BEC by the so-called Maxwell decoder. This decoder bridges the gap between BP and MAP decoding by augmenting the BP decoder with an additional "guessing" device. Analytically, the relationship between BP and MAP decoding is given in terms of the so-called extended BP EXIT (EBP EXIT) function. Fig. 1 shows this curve (double "S"-shaped curve) for transmission over the BEC and the ensemble LDPC($\frac{3x+3x^2+4x^{13}}{10}, x^6$) (the degree distributions are from an edge perspective). The BP EXIT curve is the "envelope" of the EBP EXIT curve (let a ball run slowly down the slope). The MAP EXIT curve on the other hand is conjecture to be derived in general from the EBP EXIT curve by the so-called Maxwell construction. This Maxwell construction consists of converting the EBP EXIT curve into a single-valued function by "cutting" the EBP EXIT curve at the two "S"-shaped spots in such a way that there is a local balance of the cut areas. A detailed discussion of this relationship in the case of transmission over the BEC can be found in [5]. Let us summarize. For transmission over the BEC using sparse graph codes from long ensembles, BP decoding is asymptotically characterized by its BP EXIT curve and MAP decoding is characterized by its MAP EXIT curve. These two curves are linked via the EBP EXIT curve.

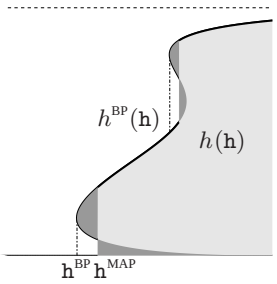

Fig. 1. The EBP EXIT curve (double "S"-shaped curve), the corresponding BP EXIT curve (dashed and solid line; the "envelope" of the EBP EXIT curve) and the MAP EXIT curve (thick solid line; constructed by "cutting" EBP EXIT at the two "S"-shaped spots in such a way that there is a local balance of the areas shown in gray) for the ensemble LDPC($\frac{3x+3x^2+4x^{13}}{10}, x^6$).

A. Overview of Results

The pleasing picture shown in Fig. 1 seems to have a fairly complete analog in the general setting. Unfortunately we are not able to prove this claim in any generality. But we show how several of the key ingredients can be suitably extended to the general case and we will be able to prove some of their fundamental properties.

Namely, we introduce a general area theorem (GAT). This area theorem, when applied to the BEC, leads back to the notion of EXIT functions as shown in the companion paper [5]. For the general case however, it is necessary to use a distinct function (but similar in many respects to EXIT). We call it the generalized EXIT (GEXIT) function. We then show that GEXIT functions share some of the key properties with EXIT functions. In particular, we are able to extend the upper-bound on the MAP threshold presented in [3] (or, more generally, the lower bound on the conditional entropy) to general channels.

In [6], [7] Guo, Shamai and Verdú showed that for Gaussian channels the derivative (with respect of the signal-to-noise ratio) of the mutual information, is equal to the mean square

† EPFL, School for Computer and Communication Sciences, CH-1015 Lausanne, Switzerland. E-mail: cyril.measson@epfl.ch

∗ ENS, Laboratoire de Physique Théorique, F-75231 Paris, France. E-mail: montanar@lpt.ens.fr

+ Flarion Technologies, Bedminster, USA E-mail: tjr@flarion.com

‡ EPFL, School for Computer and Communication Sciences, CH-1015 Lausanne, Switzerland. E-mail: ruediger.urbanke@epfl.ch

Parts of the material were presented in [1], [2].

error (MSE), and in [6] they showed that a similar relationship holds for Poisson channels. One can think of GEXIT functions as providing such a relationship in a more general setting (where the generalization is with respect to the admissible channel families). For some channel families, GEXIT functions have particularly nice interpretations. E.g., for Gaussian channels, we not only have the interpretation of the derivative in terms of the MSE detector, but this interpretation can be simplified even further in the binary case: the derivative of the mutual information can be seen as the "magnetization" of the system as was shown by Macris in [8]. The results in [9], which have appeared since the introduction of GEXIT functions in [1], can be reformulated to give an interpretation of GEXIT functions for the class of additive channels (see also [10]). It is likely that interpretations for other classes of channels will be found in the future.

B. Paper Outline

In Section II we review the necessary background material and in particular recall the GAT first stated in [1]. Starting from this GAT, we introduce in Section III GEXIT functions. We will see that for transmission over the BEC, GEXIT functions coincide with standard EXIT functions, but that this is no longer true for general channels. In Section V we then concentrate on LDPC ensembles. In particular we define the quantities which appear in the asymptotic setting. In Section IV we then prove one of the fundamental properties of GEXIT functions, namely that GEXIT kernels preserve the ordering implied by physical degradation. This fact is then exploited in Section VI, where we show how to compute an upper bound on the threshold under MAP decoding (or, more generally, a lower bound on the conditional entropy) by considering the BP GEXIT function, which results from the regular GEXIT function if we substitute the MAP density by its equivalent BP density. In Section VII we define extended BP GEXIT (EBP GEXIT) functions which include the unstable branches, present several examples of these function and discuss how they provide a bridge between belief propagation and maximum a posteriori decoding. Several properties of EPB GEXIT functions are discussed in Section VIII together with a numerical procedure for constructing them. We show that they satisfy an area theorem as well. Section IX presents some partial results on the smoothness and uniqueness of EBP GEXIT functions. In Section X we show the surprising fact that, in case the previously computed upper bound on the MAP threshold is tight, then the a posteriori probabilities on the bits are equal to the corresponding BP estimates. Section XI contains a proof that iterative coding systems cannot achieve reliable communication above capacity, using only density evolution and the area theorem (and not the standard Fano inequality). A matching condition for component codes of capacity achieving sequences follows. In the appendices we collect some technical derivations and a discussion of several equivalent forms of the GEXIT functions for Gaussian channels. We finally conclude with some remarks in Section XII.

II. Review and Notations

Let $\mathcal{X}$ denote the channel input alphabet (which we always assume finite) and $\mathcal{Y}$ the channel output alphabet (typically, $\mathcal{Y} = \mathbb{R}$). All channels considered in this paper are *memoryless* (M). Rather than looking at a single memoryless channel, we usually consider *families* of memoryless channels parameterized by a real-valued parameter ϵ, which we denote by $\{\mathrm{M}(\epsilon)\}_\epsilon$. Each channel from such a family is characterized by its transition probability density $p_{Y\,|\,X}(y\,|\,x)$ (where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$). We adopt here the convention of formally denoting channels by their transition density even when such a density does not exist, and write $\int f(y) p_{Y\,|\,X}(y\,|\,x)\mathrm{d}y$ as a proxy for the corresponding expectation.

Transmission over *binary*-input *memoryless* output-*symmetric*[1] (BMS) channel plays a particularly important role. In this case, it will be convenient to assume that the input bit X_i takes values $x_i \in \mathcal{X} \stackrel{\Delta}{=} \{+1, -1\}$. The channel indexed by parameter ϵ is generically denoted by $\mathrm{BMS}(\epsilon)$.

In the sequel we will often assume that the *channel* family $\{\mathrm{BMS}(\epsilon)\}_\epsilon$ is *ordered by physical degradation* (see [11] for a discussion of this concept). It is well known that the standard families $\{\mathrm{BEC}(\epsilon)\}_{\epsilon=0}^{1}$ (binary erasure channels with erasure parameter ϵ), $\{\mathrm{BSC}(\epsilon)\}_{\epsilon=0}^{\frac{1}{2}}$ (binary symmetric channels with cross-over probability ϵ), and $\{\mathrm{BAWGNC}(\sigma)\}_{\sigma=0}^{\infty}$ (binary-input additive white Gaussian noise channels $Y = X + N$ where X takes values in $\mathcal{X}$ and the noise N has standard deviation σ and zero-mean) all have this property. For notational simplicity we will use a shorthand and say that a channel family is *degraded*.

In the binary case, an important role is played by the distribution of the log-likelihood ratio $L \stackrel{\Delta}{=} \log \frac{p_{Y|X}(Y|+1)}{p_{Y|X}(Y|-1)}$, assuming $X = 1$. We denote the corresponding density by $\mathsf{c}(l)$ and call it an L-density. In fact, without loss of generality we can assume that the log-likelihood ratio (L) mapping, $y \mapsto \log \frac{p_{Y|X}(y|+1)}{p_{Y|X}(y|-1)}$, is already included in the channel description. This is justified since the random variable L constitutes a sufficient statistic. This inclusion of the L-processing is equivalent to assuming that $p_{Y|X}(y|+1) = \mathsf{c}(l)$. Further facts regarding BMS channels can be found in [11]. As far as LDPC and iterative coding systems are concerned, we will keep the formalism introduced in the companion paper [5] and which is found, e.g., in [12]–[15].

In the case of a *non-binary* input alphabet $\mathcal{X}$, the log-likelihood mapping will be replaced by the 'canonical' representation of the channel output $y \mapsto \nu(y) \stackrel{\Delta}{=} \{p_{Y|X}(y|x)/z(y) : x \in \mathcal{X}\}$, where $z(y) \stackrel{\Delta}{=} \sum_{x\in\mathcal{X}} p_{Y|X}(y|x)$. Notice that $\nu(y)$ belongs to the $(|\mathcal{X}|-1)$-dimensional simplex $S_{|\mathcal{X}|-1}$. In the binary case, the log-likelihood ratio is just a particular parametrization of the one-dimensional simplex.

In what follows we will often be concerned with how certain quantities (e.g., the conditional entropy $H(X\,|\,Y)$) behave as we change the channel parameter. In order to ensure that

[1] A binary memoryless channels is said to be symmetric (or, more precisely, output-symmetric) when the transition probability verifies $p_{Y|X}(y|+1) = p_{Y|X}(y|-1)$.

the involved objects exits we need to impose some regularity conditions on the channel family with respect to the channel parameter. This can be done in various ways, but to be concrete we will impose the following restriction.

Definition 1 (Channel Smoothness): Consider a family of memoryless channels with input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, and characterized by their transition probability $p_{Y|X}(y|x)$ (with y taking the canonical form described above). Assume that the family is parameterized by ϵ, where ϵ takes values in some interval $I \subseteq \mathbb{R}$. The channel family is said to be *smooth* with respect to the parameter ϵ if for all $x \in \mathcal{X}$ and all bounded continuously differentiable functions $f(y)$ on $S_{|\mathcal{X}|-1}$, the integral $\int f(y)p_{Y|X}(y|x)\mathrm{d}y$ exists and is a continuously differentiable function with respect to ϵ, $\epsilon \in I$. In the sequel we often say as a shorthand that a *channel* $\mathrm{BMS}(\epsilon)$ is smooth to mean that we are transmitting over the channel $\mathrm{BMS}(\epsilon)$ and that the *channel family* $\{\mathrm{BMS}(\epsilon)\}_\epsilon$ is smooth at the point ϵ. If $\mathrm{BMS}(\epsilon)$ is smooth, the derivative $\frac{\mathrm{d}}{\mathrm{d}\epsilon}\int f(y)p_{Y|X}(y|x)\mathrm{d}y$ exists and is a linear functional of f. It is therefore consistent to formally *define* the derivative of $p_{Y|X}(y|x)$ with respect to ϵ by setting

$$\frac{\mathrm{d}}{\mathrm{d}\epsilon}\int f(y)p_{Y|X}(y|x)\,\mathrm{d}y \triangleq \int f(y)\frac{\mathrm{d}p_{Y|X}(y|x)}{\mathrm{d}\epsilon}\,\mathrm{d}y\,. \qquad (1)$$

For a large class of channel families it is straightforward to check that they are smooth. This is e.g. the case if $\{\mathcal{Y}\}$ is finite and the transition probabilities are differentiable functions of ϵ, or if it admits a density with respect to the Lebesgue measure, and the density is differentiable for each y. In these cases, the formal derivative (1) coincides with the ordinary derivative.

Example 1 (Smooth Channels): It is straightforward to check that the families $\{\mathrm{BEC}(\epsilon)\}_{\epsilon=0}^{1}$, $\{\mathrm{BSC}(\epsilon)\}_{\epsilon=0}^{\frac{1}{2}}$, and $\{\mathrm{BAWGNC}(\sigma)\}_{\sigma=0}^{\infty}$ are all smooth.

In the case of transmission over a BMS channel it is useful to parameterize the channels in such a way that the parameter reflects the channel entropy. More precisely, we denote by $\mathtt{h}$ the conditional entropy $H(X|Y)$ when the channel input X is chosen uniformly at random from $\{+1,-1\}$, and the corresponding output is Y. Consider a family of BMS channels characterized by their L-densities. We then write this family of L-densities as $\{\mathsf{c}_\mathtt{h}\}_\mathtt{h}$ if $H(\mathsf{c}_\mathtt{h}) = \mathtt{h}$, where the *entropy operator* is defined as (see, e.g., [11])

$$H(\mathsf{c}) \triangleq \int_{-\infty}^{\infty}\mathsf{c}(y)\log_2(1+e^{-y})\mathrm{d}y = \int_{-\infty}^{\infty}\mathsf{c}(y)l(y)\mathrm{d}y. \quad (2)$$

This integral always exists as can be seen by writing it in the equivalent form as Rieman-Stieltjes integral $\int_0^\infty h_2\left(\frac{e^{-y}}{1+e^{-y}}\right)\mathrm{d}|\mathsf{C}|(y)$. In the above definition we have introduced the *kernel* $l(y) \triangleq \log_2(1+e^{-y})$. For reasons that will become clearer in Lemma 1, we call $l(y)$ the EXIT kernel.

The channel family is said to be *complete* if $\mathtt{h}$ ranges from 0 to 1. For the binary erasure channel the natural parameter ϵ (the erasure probability) already represents an entropy. Nevertheless, to be consistent we will write in the future $\mathrm{BEC}(\mathtt{h})$. By some abuse of notation, we write $\mathrm{BSC}(\mathtt{h})$ to denote the BSC with cross-over probability equal to $\epsilon(\mathtt{h}) = h_2^{-1}(\mathtt{h})$, where $h_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x)$, the binary entropy function. In the same manner, $\mathrm{BAWGNC}(\mathtt{h})$ denotes the BAWGNC with a standard deviation of the noise such that the channel entropy is equal to $\mathtt{h}$.

We will encounter cases where it is useful to allow each bit of a codeword to be transmitted through a different (family of) BMS channel(s). By some abuse of notation, we will denote the i^{th} channel family by $\{\mathrm{BMS}(\mathtt{h}_i)\}_{\mathtt{h}_i}$. A situation in which this more general view appears naturally is when we consider punctured ensembles. We can describe this case by assuming that some bits are passed through an erasure channel with erasure probability equal to one, whereas the remaining bits are passed through some other BMS channel. In such cases it is convenient to assume that all individual families $\{\mathrm{BMS}(\mathtt{h}_i)\}_{\mathtt{h}_i}$ are parameterized in a smooth (differentiable) way by a single real parameter, call it ϵ, i.e., $\mathtt{h}_i = \mathtt{h}_i(\epsilon)$. In this way, by changing ϵ all channels change according to $\mathtt{h}_i(\epsilon)$ and they describe a path through "channel space".

The general area theorem (GAT), first introduced in [1], plays center stage in the remainder of this paper.

Theorem 1 (General Area Theorem): Let X be chosen with probability $p_X(x)$ from $\mathcal{X}^n$. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i through the smooth family $\{\mathrm{M}(\epsilon_i)\}_{\epsilon_i}$, $\epsilon_i \in I_i$. Let Ω be a further observation of X so that $p_{\Omega\,|\,X,Y}(\omega\,|\,x,y) = p_{\Omega\,|\,X}(\omega\,|\,x)$. Then

$$\mathrm{d}H(X\,|\,Y,\Omega) = \sum_{i=1}^{n}\frac{\partial H(X_i\,|\,Y,\Omega)}{\partial\epsilon_i}\mathrm{d}\epsilon_i. \qquad (3)$$

Proof: For $i \in [n]$, the entropy rule gives $H(X\,|\,Y,\Omega) = H(X_i\,|\,Y,\Omega) + H(X_{\sim i}\,|\,X_i,Y,\Omega)$. We claim that

$$p(X_{\sim i}\,|\,X_i,Y,\Omega) = p(X_{\sim i}\,|\,X_i,Y_{\sim i},\Omega), \qquad (4)$$

which is true since the channel is memoryless and $p_{\Omega\,|\,X,Y}(\omega\,|\,x,y) = p_{\Omega\,|\,X}(\omega\,|\,x)$. Furthermore $H(X_i\,|\,Y,\Omega)$ is differentiable with respect to ϵ_i as a consequence of the channel smoothness (it is straightforward to write the conditional entropy as expectation of a differentiable kernel, cf. Lemma 2 and remarks below). Therefore, $H(X_{\sim i}\,|\,X_i,Y,\Omega) = H(X_{\sim i}\,|\,X_i,Y_{\sim i},\Omega)$ and $\frac{\partial H(X\,|\,Y,\Omega)}{\partial\epsilon_i} = \frac{\partial H(X_i\,|\,Y,\Omega)}{\partial\epsilon_i}$. From this the total derivate as stated in (3) follows immediately. ∎

III. GEXIT Functions

Let X be chosen with probability $p_X(x)$ from $\mathcal{X}^n$. Assume that the i^{th} component of X is transmitted over a memoryless erasure channel (not necessarily binary) with erasure probability ϵ_i, denote it by $\mathrm{EC}(\epsilon_i)$. Then $H(X_i\,|\,Y) = \bar{\epsilon}_i H(X_i\,|\,Y_i = X_i, Y_{\sim i}) + \epsilon_i H(X_i\,|\,Y_i =?, Y_{\sim i}) = \epsilon_i H(X_i\,|\,Y_{\sim i})$. Apply equation (3) in Theorem 1 assuming that $\epsilon_i = \epsilon$, $i \in [n]$. To remind ourselves that Y is a function of the parameter ϵ we write $Y(\epsilon)$. Then

$$\frac{1}{n}\frac{\mathrm{d}}{\mathrm{d}\epsilon}H(X\,|\,Y(\epsilon)) = \frac{1}{n}\sum_{i=1}^{n}H(X_i\,|\,Y_{\sim i}(\epsilon)).$$

The function $h_i(\epsilon) \triangleq H(X_i\,|\,Y_{\sim i}(\epsilon))$ is known in the literature as the EXIT function associated to the i^{th} bit of the given code and $h(\epsilon) \triangleq \frac{1}{n}\sum_{i=1}^{n}H(X_i\,|\,Y_{\sim i}(\epsilon))$ is the (*average*) EXIT

function.[2] We conclude that *for transmission over EC(ϵ),* $h(\epsilon) = \frac{1}{n}\frac{\mathrm{d}}{\mathrm{d}\epsilon}H(X\,|\,Y(\epsilon))$. If we integrate this relationship with respect to ϵ from 0 to 1 and note that $H(X\,|\,Y(0)) = 0$ and $H(X\,|\,Y(1)) = H(X)$, then we get the basic form of the area theorem for the EC(ϵ): $\int_0^1 h(\epsilon)\mathrm{d}\epsilon = H(X)/n$. This statement was first proved, in the binary case, by Ashikhmin, Kramer, and ten Brink in [16] using a different framework.

Example 2 (Area Theorem for Repetition Code and BEC): Consider the *binary* repetition code with parameters $[n, 1, n]$, where the first component describes the blocklength, the second component denotes the dimension of the code, and the final component gives the minimum (Hamming) distance. By symmetry $h_i(\mathtt{h}) = h(\mathtt{h}) = \mathtt{h}^{n-1}$ for all $i \in [n]$. We have $\int_0^1 h(\mathtt{h})\mathrm{d}\mathtt{h} = \frac{1}{n} = H(X)/n$, as predicted.
The above scenario can easily be generalized by allowing the various components of the code to be transmitted over different erasure channels. Consider, e.g., a binary repetition code of length n in which the first component is transmitted through BEC(δ), where δ is constant, but the remaining components are passed through BEC($\mathtt{h}$). In this case we have $\int_0^1 h(\mathtt{h})\mathrm{d}\mathtt{h} = (H(X\,|\,Y(\delta, 1, \cdots, 1)) - H(X\,|\,Y(\delta, 0, \cdots, 0)))/n = \delta/n$ (assuming that X is chosen uniformly at random from the set of codewords). We will get back to this point shortly when we introduce GEXIT functions in Definition 3.

The concept of EXIT functions extends to general channels in the natural way. To simplify notation somewhat let us focus on the binary case.

Definition 2 (h for BMS Channels): Let X be a binary vector of length n chosen with probability $p_X(x)$. Assume that transmission takes place over the family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Then

$$h_i(\mathtt{h}) \triangleq H(X_i\,|\,Y_{\sim i}(\mathtt{h})),$$
$$h(\mathtt{h}) \triangleq \frac{1}{n}\sum_{i=1}^{n} H(X_i\,|\,Y_{\sim i}(\mathtt{h})) = \frac{1}{n}\sum_{i=1}^{n} h_i(\mathtt{h}).$$

This is the definition of the EXIT function introduced by ten Brink [17]–[21] (see footnote 2).

We get a more explicit representation if we consider transmission using binary *linear* codes. In this context recall that a binary linear code is *proper* if it possess a generator matrix with no zero columns. As a consequence, in a proper binary linear code half the codewords take on the value $+1$ and half the value -1 in each given position.

Lemma 1 (h for Linear Codes and BMS Channels): Let X be chosen uniformly at random from a proper binary linear code and assume that transmission takes place over the family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Define

$$\phi_i(y_{\sim i}) \triangleq \log\Big(\frac{p_{X_i\,|\,Y_{\sim i}}(+1\,|\,y_{\sim i})}{p_{X_i\,|\,Y_{\sim i}}(-1\,|\,y_{\sim i})}\Big), \tag{5}$$

and $\Phi_i \triangleq \phi_i(Y_{\sim i})$. Let $\mathtt{a}_i$ denote the density of Φ_i, assuming that the all-one codeword was transmitted, and let $\mathtt{a} \triangleq \frac{1}{n}\sum_{i=1}^{n}\mathtt{a}_i$. Then

$$h_i(\mathtt{h}) = H(\mathtt{a}_i), \qquad h(\mathtt{h}) = H(\mathtt{a}),$$

where $H(\cdot)$ is the entropy operator introduced in (2).

Proof: Note that $X_i \to \Phi_i \to Y_{\sim i}$ forms a Markov chain.[3] Equivalently, we claim that Φ_i is a sufficient statistic for X_i. From this we conclude that (see [22, Section 2.8])

$$H(X_i\,|\,Y_{\sim i}) = H(X_i\,|\,\Phi_i).$$

Now note that since we assume that X was chosen uniformly at random from a proper binary linear codes, it follows that the prior for each X_i is the uniform one. Therefore, Φ_i is in fact a log-likelihood ratio. It is shown in [11, Lemma 3.37] that, assuming that X is chosen uniformly at random from a proper binary linear code, the binary "channel" $p(\phi_i\,|\,x_i)$ is symmetric. Further, note that the density of Φ_i conditioned on $X_i = 1$ is equal to the density of Φ_i conditioned that the all-one codeword was transmitted.[4] By assumption this L-density is equal to $\mathtt{a}_i$. We conclude that $H(X_i\,|\,\Phi_i) = H(\mathtt{a}_i)$. ∎

As the next example shows, the EXIT function does *not* fulfill the area theorem in the general case.

Example 3 (EXIT Function for General BMS Channels): Fig. 2 shows the EXIT function for the $[3, 1, 3]$ repetition code as well as for the $[6, 5, 2]$ single parity-check code for BEC($\mathtt{h}$), BSC($\mathtt{h}$), and BAWGNC($\mathtt{h}$). E.g., the EXIT function for the $[n, n-1, 2]$ single parity-check code over BSC($\mathtt{h}$) is given by

$$h_i(\mathtt{h}) = h(\mathtt{h}) = h_2\Big(\frac{1-(1-2\epsilon(\mathtt{h}))^{n-1}}{2}\Big),$$

where $\epsilon(\mathtt{h}) = h_2^{-1}(\mathtt{h})$. Note that these EXIT functions are "ordered." More precisely, for a repetition code we get the highest extrinsic entropy at the output for the channel family $\{\mathrm{BSC}(\mathtt{h})\}_{\mathtt{h}}$ and we get the lowest such entropy if we use instead the family $\{\mathrm{BEC}(\mathtt{h})\}_{\mathtt{h}}$. Indeed, one can show that these two families are the *least* and *most* "informative" family of channels over the whole class of BMS channels for a repetition code, [23]–[25]. The roles are exactly exchanged at a check node. Since we know that the EXIT function for the BEC fulfills the area theorem, it follows from this extremality properties that the EXIT functions for the BSC and the BAWGNC do *not* fulfill the area theorem. Indeed, for a single parity-check code with $n = 3$ and the BSC($\mathtt{h}$) the area under the EXIT function is given by

$$\int_0^1 h_2\left(\frac{1-(1-2\epsilon(\mathtt{h}))^2}{2}\right)\mathrm{d}\mathtt{h} \approx 0.643704 < 2/3.$$

Although the above fact might be disappointing it is not surprising. As it should be clear from the discussion at the

[2] More precisely, EXIT functions are usually defined as $I(X_i\,|\,Y_{\sim i}(\epsilon)) = H(X_i) - H(X_i\,|\,Y_{\sim i}(\epsilon))$, which differs from our definition only in a trivial way.

[3] For $z \in \mathbb{R}$, let $y_{\sim i}$ be an element of $\big(\phi_i\big)^{-1}(z)$ so that $z = \phi_i(y_{\sim i})$. Then $p_{X_i\,|\,Y_{\sim i},\Phi_i}(x_i\,|\,y_{\sim i}, z) = \frac{(1+x_i)+(1-x_i)e^z}{2(1+e^z)} = p_{X_i\,|\,\Phi_i}(x_i\,|\,z)$. From this we conclude that $p_{Y_{\sim i}\,|\,X_i,\Phi_i}(y_i\,|\,x_{\sim i}, z) = p_{Y_{\sim i}\,|\,\Phi_i}(y_{\sim i}\,|\,z)$.

[4] To see this, note that, using the symmetry of the channel and the equal prior on the codewords, we can write $p_{X_i\,|\,Y}(x_i\,|\,y) = c(y)\sum_{\tilde{x}\in\mathcal{C}:\tilde{x}_i=x_i} p_{Y\,|\,X}(y\tilde{x}\,|\,\underline{1})$, where $c(y)$ is a constant independent of x_i, $\mathcal{C}$ denotes the code, and $\underline{1}$ denotes the all-one codeword. In the same manner, if $x' \in \mathcal{C}$, then $p_{X_i\,|\,Y}(x_i\,|\,yx') = c'(y)\sum_{\tilde{x}\in\mathcal{C}:\tilde{x}_i=x_i x'_i} p_{Y\,|\,X}(yx'\tilde{x}\,|\,x')$. Compare the density of the log-likelihood ratio assuming that the all-one codeword was transmitted to the one assuming that the codeword x' was transmitted. The claim follows by noting that for any $y \in \mathcal{Y}$, $p_{Y\,|\,X}(y\,|\,\underline{1}) = p_{Y\,|\,X}(yx'\,|\,x')$, and that in this case also $p_{Y\,|\,X}(y\tilde{x}\,|\,\underline{1}) = p_{Y\,|\,X}(yx'\tilde{x}\,|\,x')$.

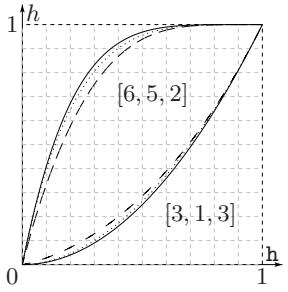

Fig. 2. The EXIT function of the $[3,1,3]$ repetition code and the $[6,5,2]$ parity-check code for the BEC($\mathtt{h}$) (solid curve), BSC($\mathtt{h}$) (dashed curve) and BAWGNC($\mathtt{h}$) (dotted curve).

beginning of this section, the EXIT function is related to the GAT only in the case of the erasure channel. Let us therefore go back to the GAT and *define* the function which fulfills the area theorem in the general case.

Definition 3 (GEXIT Function): Let X be a vector of length n chosen with probability $p_X(x)$ from $\mathcal{X}^n$. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i through the smooth family $\{\mathrm{M}(\epsilon_i)\}_{\epsilon_i}$, $\epsilon_i \in [0,1]$. Assume that all individual channels are parameterized in a smooth (differentiable) way by a common parameter ϵ, i.e., $\epsilon_i = \epsilon_i(\epsilon)$, $i \in [n]$. Let Ω be a further observation of X so that $p_{\Omega\,|\,X,Y}(\omega\,|\,x,y) = p_{\Omega\,|\,X}(\omega\,|\,x)$. Then the i^{th} and the (average) *generalized* EXIT (GEXIT) function are defined by

$$g_i(\epsilon) \triangleq \frac{\partial H(X_i|Y,\Omega)}{\partial \epsilon_i}\frac{\mathrm{d}\epsilon_i}{\mathrm{d}\epsilon}\Big|_{\epsilon},$$
$$g(\epsilon) \triangleq \frac{1}{n}\sum_{i=1}^{n} g_i(\epsilon).$$

Discussion: The definition is stated in quite general terms. First note that if we consider the integral $\int_{\underline{\epsilon}}^{\overline{\epsilon}} g(\epsilon)\mathrm{d}\epsilon$, then from Theorem 1 we conclude that the result is $\frac{1}{n}\big(H(X\,|\,Y(\overline{\epsilon}),\Omega) - H(X\,|\,Y(\underline{\epsilon}),\Omega)\big)$. In words, if we smoothly change the individual channel parameters ϵ_i as a function of ϵ, then the integral of $g_i(\epsilon)$ tells us how much the conditional entropy of the system changes due to the total change of the parameters ϵ_i. To be concrete, assume, e.g., that all bits are sent through Gaussian channels. We can imagine that we first only change the parameter of the Gaussian channel through which bit 1 is sent from its initial to its final value, then the parameter of the second channel and so on. Alternatively, we can imagine that all channel parameters are changed simultaneously. In the two cases the integrals of the individual GEXIT functions g_i differ but their sum is the same and it equals the total change of the conditional entropy due to the change of channel parameters. Therefore, GEXIT functions can be considered to be a "local" way of measuring the change of the conditional entropy of a system. One should think of the common parameter ϵ as a convenient way of parameterizing the path through "channel space" that we are taking.

In many applications all channels are identical, and formulas simplify significantly. In Section VII we will see a case in which the extra degree of freedom afforded by allowing different channels is important. The additional observation Ω is useful if we consider the design or iterative systems and component-wise GEXIT functions. For what follows though we will not need it. Hence, we will drop Ω in the sequel.

If we assume that the input is *binary* we obtain a more explicit expression for the GEXIT functions.

Lemma 2 (g for BM Channels): Let X be a *binary* vector of length n chosen with probability $p_X(x)$. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i over the smooth family $\{\mathrm{BM}(\mathtt{h}_i)\}_{\mathtt{h}_i}$, $\mathtt{h}_i \in [0,1]$. Assume that all individual channel families are parameterized in a smooth (differentiable) way by a common parameter ϵ, i.e., $\mathtt{h}_i = \mathtt{h}_i(\epsilon)$, $i \in [n]$. Then the i^{th} and the (average) *generalized* EXIT (GEXIT) function are given by

$$g_i(\epsilon) = \int_{\phi_i,y_i}\sum_{x_i} p(x_i)p(\phi_i\,|\,x_i)\frac{\mathrm{d}}{\mathrm{d}\mathtt{h}_i}p(y_i|x_i)\cdot \tag{6}$$
$$\cdot\log\left\{\sum_{x_i'}\frac{p(x_i'|\phi_i)p(y_i|x_i')}{p(x_i|\phi_i)p(y_i|x_i)}\right\}\frac{\mathrm{d}\mathtt{h}_i}{\mathrm{d}\epsilon}\mathrm{d}y_i\mathrm{d}\phi_i,$$
$$g(\epsilon) = \frac{1}{n}\sum_{i=1}^{n} g_i(\epsilon), \tag{7}$$

where $\phi_i(y_{\sim i})$ and Φ_i are defined as in (5).
Discussion: As mentioned above, the derivative of $p(y_i|x_i)$ in Eq. (6) has to be interpreted in general as in Eq. (1). Moreover, writing the same expression as $g_i(\epsilon) = \int f(y)\frac{\mathrm{d}}{\mathrm{d}\mathtt{h}_i}p(y_i|x_i)\mathrm{d}y$, the existence of such derivative follows from the channel smoothness and the differentiability of $f(y)$ (if written as a function of the log-likelihood $\log\frac{p(y|+1)}{p(y|-1)}$.

Proof: We proceed as in the proof of Lemma 1. We claim that $X_i \to (\Phi_i, Y_i) \to Y$ forms a Markov chain (equivalently, (Φ_i, Y_i) constitutes a sufficient statistic). To see this, fix $z \in \mathbb{R}$ and let $y_{\sim i}$ be an element of $\big(\phi_i\big)^{-1}(z)$, so that $z = \phi_i(y_{\sim i})$. Then, using the fact that Y_i is conditionally independent of $Y_{\sim i}$, given $X_i = x_i$, we may write

$$p_{X_i\,|\,Y_i,Y_{\sim i},\Phi_i}(x_i\,|\,y_i,y_{\sim i},z) = \frac{p_{Y_i\,|\,X_i}(y_i\,|\,x_i)p_{X_i\,|\,Y_{\sim i},\Phi_i}(x_i\,|\,y_{\sim i},z)}{\sum_{x_i'\in\mathcal{X}} p_{Y_i\,|\,X_i}(y_i|x_i')p_{X_i\,|\,Y_{\sim i},\Phi_i}(x_i'\,|\,y_{\sim i},z)}$$

Since $X_i \to \Phi_i \to Y_{\sim i}$ forms a Markov chain (as already shown in the proof of Lemma 1), we have $p_{X_i\,|\,Y_{\sim i},\Phi_i}(x_i\,|\,y_{\sim i},z) = p_{X_i\,|\,\Phi_i}(x_i\,|\,z)$. Substituting in the above equation, we get $p_{X_i\,|\,Y_i,Y_{\sim i},\Phi_i}(x_i\,|\,y_i,y_{\sim i},z) = p_{X_i\,|\,Y_i,\Phi_i}(x_i\,|\,y_i,z)$, as claimed.

Therefore, we can rewrite $g_i(\epsilon)$ as

$$g_i(\epsilon) = \frac{\partial H(X_i|Y)}{\partial \mathtt{h}_i}\frac{\mathrm{d}\mathtt{h}_i}{\mathrm{d}\epsilon}\Big|_{\epsilon} = \frac{\partial H(X_i|\Phi_i,Y_i)}{\partial \mathtt{h}_i}\frac{\mathrm{d}\mathtt{h}_i}{\mathrm{d}\epsilon}\Big|_{\epsilon}.$$

Expand $H(X_i|\Phi_i,Y_i)$ as

$$-\int_{\phi_i,y_i}\sum_{x_i} p(x_i,\phi_i,y_i)\log_2(p(x_i\,|\,\phi_i,y_i))\mathrm{d}y_i\mathrm{d}\phi_i$$
$$= -\int_{\phi_i,y_i}\sum_{x_i} p(x_i)p(\phi_i\,|\,x_i)p(y_i|x_i)\cdot$$
$$\cdot\log_2\left\{\frac{p(x_i|\phi_i)p(y_i|x_i)}{\sum_{x_i'\in\mathcal{X}} p(x_i'|\phi_i)p(y_i|x_i')}\right\}\mathrm{d}y_i\mathrm{d}\phi_i.$$

This form has the advantage that the dependence of $H(X_i|\Phi_i,Y_i)$ upon the channel at position i is completely

explicit. Let us therefore differentiate the above expression with respect to $\mathtt{h}_i$, the parameter which governs the transition probability $p(y_i \,|\, x_i)$. The terms obtained by differentiating with respect to the channel *inside* the $\log_2$ vanish. For instance, when differentiating with respect to the $p(y_i|x_i)$ at the numerator, we get

$$-\int_{\phi_i,y_i}\sum_{x_i} p(x_i)p(\phi_i \,|\, x_i)\frac{\mathrm{d}}{\mathrm{d}\mathtt{h}_i}p(y_i \,|\, x_i)\mathrm{d}y_i\mathrm{d}\phi_i$$
$$=-\int_{\phi_i}\sum_{x_i} p(x_i)p(\phi_i \,|\, x_i)\frac{\mathrm{d}}{\mathrm{d}\mathtt{h}_i}\int_{y_i} p(y_i \,|\, x_i)\mathrm{d}y_i\mathrm{d}\phi_i = 0\,.$$

When differentiating with respect to the *outer* $p(y_i|x_i)$ we get the stated result. ∎

Although the last lemma was stated for the case of binary channels, it poses no difficulty to generalize it. It is in fact sufficient to replace $\phi_i(y_{\sim i})$ with any sufficient statistic of X_i, given $Y_{\sim i} = y_{\sim i}$. For instance, one may take $\phi_i(y_{\sim i}) = \{p_{X_i|Y_{\sim i}}(x_i \,|\, y_{\sim i});\ x_i \in \mathcal{X}\}$, which takes value on the $(|\mathcal{X}|-1)$-dimensional simplex, or any parameterization of it. The log-likelihood can be regarded as a particular parameterization of the 1-dimensional simplex. More generally, $p_{X_i|Y_{\sim i}}(x_i \,|\, y_{\sim i})$ is a natural quantity appearing in iterative decoding. The proof (as well as the statement) applies verbatimly to this case.

We get an even more compact description if we assume that transmission takes place using a binary *proper linear* code and that the channel is *symmetric*.

Lemma 3 (g for Linear Codes and BMS Channels): Let X be chosen uniformly at random from a proper binary linear code of length n. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i over the smooth family $\{\mathrm{BMS}(\mathtt{h}_i)\}_{\mathtt{h}_i}$. Assume that all individual channels are parameterized in a smooth (differentiable) way by a common parameter ϵ, i.e., $\mathtt{h}_i = \mathtt{h}_i(\epsilon)$, $i \in [n]$. Let the i^{th} channel be characterized by its L-density, which by some abuse of notation we denote by $\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}$. Let ϕ_i and Φ_i be as defined in (5) and let a_i denote the density of Φ_i, assuming that the all-one codeword was transmitted. Then

$$g_i(\epsilon) = \int_{-\infty}^{\infty} \mathsf{a}_i(z) l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}}(z)\ \mathrm{d}z,$$

where

$$l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}}(z) \triangleq \int_{-\infty}^{\infty} \frac{\partial \mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)}{\partial \epsilon}\log_2(1+\mathrm{e}^{-z-w})\ \mathrm{d}w.$$

Discussion: The remarks made after Lemma 2 apply in particular to the present case: We write $\int_{-\infty}^{\infty}\frac{\partial \mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)}{\partial\epsilon}\log_2(1+\mathrm{e}^{-z-w})\ \mathrm{d}w$ as a proxy for $\frac{\partial}{\partial\epsilon}\left\{\int_{-\infty}^{\infty}\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)\log_2(1+\mathrm{e}^{-z-w})\ \mathrm{d}w\right\}$. The latter expression exists, since $\log_2(1+\mathrm{e}^{-z-w})$ is continuously differentiable as a function of w and by assumption the channel family is smooth. Note further that $l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}}(z)$ is continuous and non-negative so that $g_i(\epsilon)$ exists as well.

Proof: Consider the expression for $g_i(\epsilon)$ as given in (7). By assumption, $p(y_i \,|\, x_i)$ is symmetric for all $i \in [n]$. Further, as already remarked in the proof of Lemma 1, the "channel" $p(\phi_i \,|\, x_i)$ is symmetric as well. It follows from this and the fact that $p_{X_i}(+1) = p_{X_i}(-1)$ (due to the assumption that the code is proper and that codewords are chosen with uniform probability) that the contributions to $g_i(\epsilon)$ for $x_i = +1$ and $x_i = -1$ are identical. We can therefore assume without loss of generality that $x_i = +1$. Recall that the density of Φ_i assuming that $X_i = 1$ is equal to the density of Φ_i assuming that the all-one codeword was transmitted. The latter is by definition equal to a_i. As remarked earlier, a_i is symmetric. Further, as discussed in the introduction, we can assume that the i^{th} BMS channel outputs already log-likelihood ratios. Therefore, $p_{Y_i|X_i}(y_i|+1) = \mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(y_i)$. Finally, consider the expression within the $\log_2$. If $x_i' = +1$ then the numerator and denominator are equal and we get one. If on the other hand $x_i' = -1$ then we get by the previous remarks the product of the likelihoods. Putting this all together we get

$$g_i(\epsilon) = \int \mathsf{a}_i(z)\frac{\mathrm{d}\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)}{\mathrm{d}\mathtt{h}_i}\log_2\left(1+\mathrm{e}^{-z-w}\right)\mathrm{d}z\mathrm{d}w.$$

The thesis follows by rearranging terms. ∎

Example 4 (Alternative Kernel Representations): Note that because of the symmetry property of L-densities we can write

$$g(\epsilon) = \int_{-\infty}^{\infty}\mathsf{a}(z)l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)\ \mathrm{d}z$$
$$= \int_{0}^{\infty}|\mathsf{a}|(z)\frac{l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)+e^{-z}l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(-z)}{1+e^{-x}}\mathrm{d}z.$$

This means that the kernel is uniquely specified on the absolute value domain $[0,\infty]$, but that for each $z \in [0,\infty]$ we can split the weight of the kernel in any desired way between $+z$ and $-z$ so that $l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)+e^{-z}l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(-z)$ equals the desired value. In the sequel we will use this degree of freedom to bring some kernels into a more convenient form. Although it constitutes some abuse of notation we will in the sequel make no notational distinction between equivalent such kernels even though pointwise they might not represent the same function.

As we have already remarked in the discussion right after Definition 3, the GEXIT functions $g_i(\epsilon)$ allow us to "locally" measure the change of the conditional entropy of a system. This property is particularly apparent in the representation of Lemma 3 where we see that the local measurement has two components: (i) the kernel which depends on the derivative of the channel seen at the given position and (ii) the distribution a_i, which encapsulates all our ignorance about the code behavior with respect to the i^{th} position. This representation is very intuitive. If we improve the observation of a particular bit (derivative of the channel with respect to the parameter) then the amount by which the conditional entropy of the overall system changes clearly depends on how well this particular bit was already known via the code constraints and the observations of the other bits (extrinsic posterior density): if the bit was already perfectly known then the additional observation afforded will be useless, whereas if nothing was known about the bit one would expect that the additional reduction in entropy of this bit fully translates to a reduction of the entropy of the overall system. We will see some quantitative statements of this nature in Section IV.

In the next three examples we compute the kernels $l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}}(z)$ for the standard families $\{\mathrm{BEC}(\mathtt{h})\}_{\mathtt{h}}$, $\{\mathrm{BSC}(\mathtt{h})\}_{\mathtt{h}}$, and $\{\mathrm{BAWGNC}(\mathtt{h})\}_{\mathtt{h}}$. If we consider a single family of BMS channels parameterized by the entropy $\mathtt{h}$ it is convenient to

"normalize" the GEXIT kernel so that it measure the "progress per dh". This means, in the following examples we compute

$$l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z) \triangleq \frac{\int_{-\infty}^{\infty} \frac{\partial \mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)}{\partial \epsilon} \log_2(1+\mathrm{e}^{-z-w})\,\mathrm{d}w}{\int_{-\infty}^{\infty} \frac{\partial \mathsf{c}_{\mathrm{BMS}(\mathtt{h}_i)}(w)}{\partial \epsilon} \log_2(1+\mathrm{e}^{-w})\,\mathrm{d}w}. \quad (8)$$

Example 5 (GEXIT Kernel, L-Domain – $\{BEC(\mathtt{h})\}_{\mathtt{h}}$): If we take the family $\{\mathsf{c}_{\mathrm{BEC}(\mathtt{h})}\}_{\mathtt{h}}$, where $\mathtt{h} = \epsilon$ denotes both, the channel (intrinsic) entropy and the cross-over erasure probability, then a quick calculation shows that $l^{\mathsf{c}_{\mathrm{BEC}(\mathtt{h})}}(z) = \log_2(1+e^{-z}) = l(z)$. In words, the GEXIT kernel with respect to the family $\{\mathrm{BEC}(\mathtt{h})\}_{\mathtt{h}}$ is the regular EXIT kernel.

Example 6 (GEXIT Kernel, L-Domain – $\{BSC(\mathtt{h})\}_{\mathtt{h}}$): Let us now look at the family $\{\mathsf{c}_{\mathrm{BSC}(\mathtt{h})}\}_{\mathtt{h}}$. Some calculus shows that

$$l^{\mathsf{c}_{\mathrm{BSC}(\mathtt{h})}}(z) = \log\left(\frac{1+\frac{1-\epsilon}{\epsilon}\mathrm{e}^{-z}}{1+\frac{\epsilon}{1-\epsilon}\mathrm{e}^{-z}}\right) / \log\left(\frac{1-\epsilon}{\epsilon}\right),$$

where $\epsilon = h_2^{-1}(\mathtt{h})$. For a fixed $z \in \mathbb{R}$ and $\mathtt{h} \to 0$, the kernel converges to 1 as $1 + z/\log(\epsilon)$, whereas the limit when $\mathtt{h} \to 1$ is equal to $\frac{2}{1+e^z}$.

Example 7 (GEXIT Kernel, L-Domain – $\{BAWGNC(\mathtt{h})\}_{|ent}$): Consider now the family $\{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h})}\}_{\mathtt{h}}$, where $\mathtt{h}$ denotes the channel entropy. This family is defined in Example 1. Recall that the noise is assumed to be Gaussian with zero-mean and variance σ^2. A convenient parameterization for this case is $\epsilon \triangleq 2/\sigma^2$. This means that in the following $\mathtt{h} = H(\mathsf{c}_{\mathrm{BAWGNC}(\sigma^2=2/\epsilon)})$. After some steps of calculus shown in Appendix I and Lemma 18, we get

$$l^{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h})}}(z) = \left(\int_{-\infty}^{+\infty} \frac{\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{1+\mathrm{e}^{w+z}}\mathrm{d}w\right) / \left(\int_{-\infty}^{+\infty} \frac{\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{1+\mathrm{e}^{w}}\mathrm{d}w\right).$$

In Appendix I we give alternative representations and/or interpretations of this kernel. In particular we discuss the relationship to the formulation presented by Guo, Shamai and Verdú in [7], [26] using a connection to the MSE detector as well as the formulation by Macris in [8] based on the Nishimori identity.

One convenient feature of standard EXIT functions is that they are fairly similar for a given code across the whole range of BMS channels. Is this still true for GEXIT functions? GEXIT functions depend on the channel *both* through the kernel as well as through the extrinsic densities. Let us therefore compare the shape of the various kernels. It is most convenient to compare the kernels not in the L-domain but in the $|D|$-domain. A change of variables shows that in general the L-domain kernel, call it $l^{\mathsf{c}}(\cdot)$, and the associated $|D|$-domain kernel, denote it by $|d|^{\mathsf{c}}(\cdot)$, are linked by

$$|d|^{\mathsf{c}}(s) = \frac{1-s}{2} l^{\mathsf{c}}(\log\frac{1-s}{1+s}) + \frac{1+s}{2} l^{\mathsf{c}}(\log\frac{1+s}{1-s}). \quad (9)$$

E.g., if we apply the above transformation to the previous examples we get the following results.

Example 8 (GEXIT Kernel, $|D|$-Domain – $\{BEC(\mathtt{h})\}_{\mathtt{h}}$): We get $|d|^{\mathsf{c}_{\mathrm{BEC}(\mathtt{h})}}(s) = h_2((1+s)/2)$.

Example 9 (GEXIT Kernel, $|D|$-Domain – $\{BSC(\mathtt{h})\}_{\mathtt{h}}$): Some calculus shows that $|d|^{\mathsf{c}_{\mathrm{BSC}(\mathtt{h}(\epsilon))}}(s) = 1 + \frac{s}{\log((1-\epsilon)/\epsilon)} \log\left(\frac{1+2\epsilon s-s}{1-2\epsilon s+s}\right)$. The limiting values are seen to be $\lim_{\mathtt{h}\to 1} |d|^{\mathsf{c}_{\mathrm{BSC}(\mathtt{h})}}(s) = 1-s^2$, and $\lim_{\mathtt{h}\to 0} |d|^{\mathsf{c}_{\mathrm{BSC}(\mathtt{h})}}(s) = 1$.

Example 10 (GEXIT Kernel, $|D|$-Domain – $\{BAWGN(\mathtt{h})\}_{\mathtt{h}}$): Using Example 7 and (9), it is straightforward to write the kernel in the $|D|$-domain as

$$|d|^{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h}(\epsilon))}}(s) = \sum_{i\in\{-1,+1\}} \frac{\int_{-\infty}^{+\infty} \frac{(1-s^2)\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{(1+is)+(1-is)\mathrm{e}^{w}}\mathrm{d}w}{\int_{-\infty}^{+\infty} \frac{2\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{1+\mathrm{e}^{w}}\mathrm{d}w}.$$

As shown in Appendix I, the limiting values are the same as for the BSC, i.e., $\lim_{\mathtt{h}\to 1} |d|^{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h})}}(s) = 1-s^2$, and $\lim_{\mathtt{h}\to 0} |d|^{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h})}}(s) = 1$.

In Fig. 3 we compare the EXIT kernel (which is also the GEXIT kernel for the BEC) with the GEXIT kernels for BSC($\mathtt{h}$) and BAWGNC($\mathtt{h}$) in the $|D|$-domain for several channel parameters. Note that these kernels are distinct but quite similar. In particular, for $\mathtt{h} = 0.5$ the GEXIT kernel with respect to BAWGNC($\mathtt{h}$) is hardly distinguishable from the regular EXIT kernel. The GEXIT kernel for the BSC shows more variation.

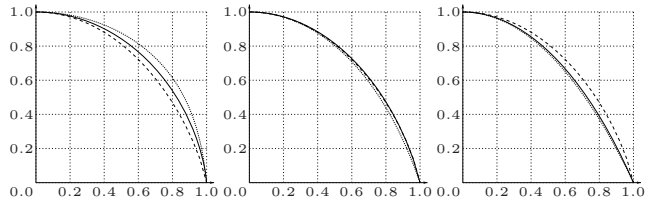

Fig. 3. Comparison of the kernels $|d|^{\mathsf{c}_{\mathrm{BEC}(\mathtt{h})}}(s)$ (dashed line) with $|d|^{\mathsf{c}_{\mathrm{BSC}(\mathtt{h})}}(s)$ (dotted line) and $|d|^{\mathsf{c}_{\mathrm{BAWGNC}(\mathtt{h})}}(s)$ (solid line) at channel entropy rate $\mathtt{h} = 0.1$ (left), $\mathtt{h} = 0.5$ (middle) and $\mathtt{h} = 0.9$ (right).

Example 11 (Repetition Code): Consider the $[n, 1, n]$ repetition code. Let $\{\mathsf{c}_{\mathtt{h}}\}_{\mathtt{h}}$ characterize a smooth family of BMS channels. For $n \in \mathbb{N}$, let $\mathsf{c}_{\mathtt{h}}^{\star n}$ denote the n-fold convolution of $\mathsf{c}_{\mathtt{h}}$. The GEXIT function for the $[n, 1, n]$ repetition code is then given by $g(\mathtt{h}) = \frac{1}{n}\frac{\mathrm{d}}{\mathrm{d}\mathtt{h}} H(\mathsf{c}_{\mathtt{h}}^{\star n})$. Explicitly, we get $g_{\mathrm{BEC}}(\mathtt{h}) = \mathtt{h}^n = h_{\mathrm{BEC}}(\mathtt{h})$. As a further example, g_{BSC} is given in parametric form by

$$\Big(h_2(\epsilon), \frac{\sum_{j=\pm 1} j \sum_{i=1}^{n} \binom{n}{i} \epsilon^i \overline{\epsilon}^{n-i} \log\big(1+(\epsilon/\overline{\epsilon})^{n-2i-j}\big)}{n \log(\overline{\epsilon}/\epsilon)}\Big),$$

with $\overline{\epsilon} = 1-\epsilon$.

Example 12 (Single Parity-Check Code): Consider the dual code, i.e., the $[n, n-1, 2]$ parity-check code. Some calculations show that g_{BSC} is given in parametric form by

$$\Big(h_2(\epsilon), 1-(1-2\epsilon)^{n-1}\frac{\log\big(\frac{1+(1-2\epsilon)^n}{1-(1-2\epsilon)^n}\big)}{\log\big(\frac{1-\epsilon}{\epsilon}\big)}\Big).$$

No simple analytic expressions are known for the case of transmission over the BAWGNC.

Fig. 4 compares EXIT to GEXIT curves for some repetition and some single parity-check codes.

Example 13 (Hamming Code): Consider the $[7, 4, 3]$ Hamming code. When transmission takes place over BEC($\mathtt{h}$), it is a tedious but conceptually simple exercise to show that the EXIT function is $h(\mathtt{h}) = 3\mathtt{h}^2 + 4\mathtt{h}^3 - 15\mathtt{h}^4 + 12\mathtt{h}^5 - 3\mathtt{h}^6$,

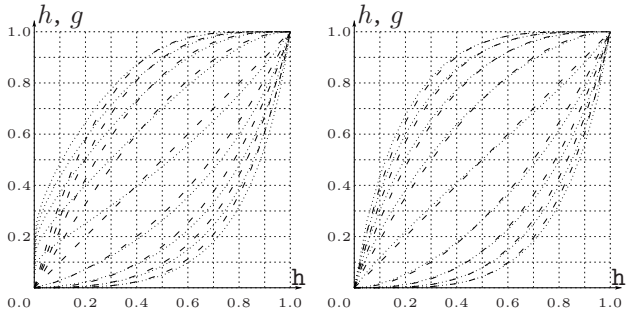

Fig. 4. The EXIT (dashed) and GEXIT (dotted) function of the $[n, 1, n]$ repetition code and the $[n, n-1, 2]$ parity-check code assuming that transmission takes place over BSC($\mathtt{h}$) (left picture) or the BAWGNC($\mathtt{h}$) (right picture), $n \in \{2, 3, 4, 5, 6\}$.

see, e.g., [3], [16]. In a similar way, using the derivative of the conditional entropy, one can give an analytic expression for the GEXIT function assuming transmission takes place over the BSC. Both expressions are evaluated in Fig. 5 (left). A comparison between GEXIT and EXIT functions for the Hamming code and the BSC is shown in Fig. 5 (right).

Example 14 (Simplex Code): Consider now the dual of the Hamming code, i.e., the $[7, 3, 4]$ Simplex code. For transmission over the BEC we have $h(\mathtt{h}) = 4\mathtt{h}^3 - 6\mathtt{h}^5 + 3\mathtt{h}^6$. Fig. 5 compares GEXIT and EXIT functions for this code when transmission takes place over the BEC and over the BSC.

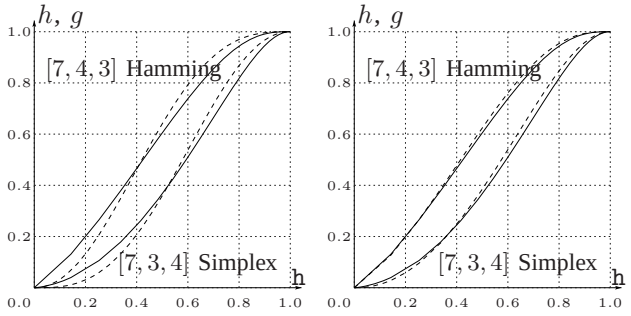

Fig. 5. Comparison of the GEXIT functions for the $[7, 4, 3]$ Hamming code and its dual. Left picture: Comparison between GEXIT functions when transmitting over the BEC (dashed line) and over the BSC (solid line). Right picture: Comparison between GEXIT (solid line) and EXIT (dashed line) functions when transmission takes place over the BSC.

IV. Basic Properties of GEXIT Functions

GEXIT functions fulfill the GAT by definition. Let us state a few more of their properties.

We first show that the GEXIT function preserves the partial order implied by physical degradation.

Lemma 4: Let X be chosen with probability $p_X(x)$ from $\mathcal{X}^n$. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i through the smooth and degraded family $\{\mathrm{M}(\epsilon_i)\}_{\epsilon_i}$, $\epsilon_i \in I_i$. If $X \to Y_{\sim i} \to \Phi_i$ forms a Markov chain then

$$\frac{\partial H(X_i \,|\, Y)}{\partial \epsilon_i} \leq \frac{\partial H(X_i \,|\, Y_i, \Phi_i)}{\partial \epsilon_i}. \tag{10}$$

Proof: Since the derivatives in Eq. (10) are known to exist a.e., the above statement is in fact equivalent to saying that, for any $\epsilon_i' \geq \epsilon_i$,

$$H(X_i \,|\, Y_i(\epsilon_i'), Y_{\sim i}) - H(X_i \,|\, Y_i(\epsilon_i), Y_{\sim i}) \leq H(X_i \,|\, Y_i(\epsilon_i'), \Phi_i) - H(X_i \,|\, Y_i(\epsilon_i), \Phi_i)\,.$$

Here, $Y_i(\epsilon_i)$ and $Y_i(\epsilon_i')$ are the result of transmitting X_i through the channels with parameter ϵ_i and ϵ_i', respectively. We claim that

$$\begin{aligned} &X \to Y_i(\epsilon_i) \to Y_i(\epsilon_i'),\\ &X \to Y_{\sim i} \to \Phi_i,\\ &(Y_i(\epsilon_i), Y_i(\epsilon_i')) \to X \to (Y_{\sim i}, \Phi_i). \end{aligned}$$

The first claim follows from the assumption that the channel family is degraded and the second claim is also part of the assumption. Finally, the third claim is true since the channel is memoryless.

The thesis is therefore a consequence of Lemma 5 stated below by making the following substitutions:

$$\begin{aligned} Y_i(\epsilon_i) &\to Y, & Y_i(\epsilon_i') &\to Y',\\ Y_{\sim i} &\to Z, & \Phi_i &\to Z'. \end{aligned}$$

■

Lemma 5: Assume that $X \to Y \to Y'$, $X \to Z \to Z'$, as well as $(Y, Y') \to X \to (Z, Z')$ form Markov chains. Then

$$H(X \,|\, Y', Z) - H(X \,|\, Y, Z) \leq H(X \,|\, Y', Z') - H(X \,|\, Y, Z')\,. \tag{11}$$

Proof: The statement is equivalent to $H(X \,|\, Z, Y', Z') - H(X \,|\, Y, Z, Y', Z') \leq H(X \,|\, Y', Z') - H(X \,|\, Y, Y', Z')$. Let us now condition on a event $(Y' = y', Z' = z')$. The proof is completed by showing that (here the conditioning upon $Y' = y', Z' = z'$ is left implicit for the sake of simplicity)

$$H(X \,|\, Y, Z) - H(X \,|\, Y) - H(X \,|\, Z) + H(X) \geq 0\,. \tag{12}$$

This inequality can be written in terms of mutual information as $I(Y; X \,|\, Z) \leq I(Y; X)$. The statement is therefore a well-known consequence of the data processing inequality, see [22, p. 33], if we can show that, conditioned on $Y' = y', Z' = z'$, $Y \to X \to Z$ forms a Markov chain. In formulae, we have to show that $p(y, z \,|\, x, y', z') = p(y \,|\, x, y', z')p(z \,|\, x, y', z')$, which in turn follows if we can show that $\frac{p(z \,|\, x, y', z')}{p(z \,|\, x, y, y', z')} = 1$. The last equality can be shown by first applying Bayes law, then expanding all terms in the order x, z', y and y', further canceling common terms and, finally, repeatedly using the conditions that $X \to Y \to Y'$, $X \to Z \to Z'$, as well as $(Y, Y') \to X \to (Z, Z')$ form Markov chains. ■

In case of linear codes, and communication over a smooth and degraded family of BMS channels, Lemma 3 provides an explicit representation of the GEXIT function in terms of L-densities. In this case Lemma 4 becomes a statement on the corresponding kernel. For completeness, let us state the corresponding condition explicitly.

Corollary 1 ($l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)$ Preserves Partial Order): Consider a smooth and degraded family of BMS channels characterized by the associated family of L-densities $\{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}\}_{\mathtt{h}}$. Let a and

b denote two symmetric L-densities so that $\mathsf{a} \prec \mathsf{b}$, i.e., b is physically degraded with respect to a. Then

$$\int_{-\infty}^{\infty} \mathsf{a}(z)\, l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)\mathrm{d}z \leq \int_{-\infty}^{\infty} \mathsf{b}(z)\, l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)\mathrm{d}z.$$

An alternative proof of this statement is provided in Appendix II.

We continue by examining some limiting cases. In the sequel $\mathfrak{E}$ denotes the error-probability operator. In the L-domain it is defined as $\mathfrak{E}(\mathsf{a}) = \frac{1}{2}\int_{-\infty}^{\infty} \mathsf{a}(z)e^{-(|z/2|+z/2)}\mathrm{d}z$.

Lemma 6 (Bounds for GEXIT Kernel): Let $|d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)$ be the kernel associated to a smooth degraded family of BMS channels characterized by their family of L-densities $\{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}\}_{\mathtt{h}}$. Then

$$1 - z \leq |d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z) \leq 1.$$

Therefore, if a is a symmetric L-density, we have

$$2\,\mathfrak{E}(\mathsf{a}) \leq \int_{-\infty}^{\infty} l^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)\mathsf{a}(z)\mathrm{d}z \leq 1\,.$$

Proof: In Appendix II, we show that $|d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z)$ is non-increasing and concave. The upper bound follows from $|d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z) < |d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z=0) = 1$. The lower bound is proved in a similar way by using concavity and observing that $|d|^{\mathsf{c}_{\mathrm{BMS}(\mathtt{h})}}(z=1) = 0$. The final claim now follows from the fact that the $|D|$-domain kernel associated to $\mathfrak{E}$ is equal to $(1-z)/2$. ∎

Lemma 7 (Further Properties of GEXIT Functions): Let $g(\mathtt{h})$ be the GEXIT function associated to a proper binary linear code of minimum distance larger than 1, and transmission over a complete smooth family of BMS channels. Then

$$g(0) = 0, \qquad g(1) = 1.$$

If the minimum distance of the code is larger than k, then

$$\frac{\mathrm{d}^{k-1}}{\mathrm{d}\mathtt{h}^{k-1}} g(\mathtt{h})\bigg|_{\mathtt{h}=0} = 0.$$

Further, $g(\mathtt{h})$ is a non-decreasing function in $\mathtt{h}$.

Proof: Consider the first two assertions. If $\mathtt{h} = 0$, then the associated L-density corresponds to a "delta at infinity" (this is an easy consequence of the minimum distance being at least 2). On the other hand, if $\mathtt{h} = 1$ then the corresponding L-density is a "delta at zero." The claim in both cases follows now by a direct calculation.

In order to prove the last claim, we use the definition of $g(\mathtt{h})$ to write

$$\frac{\mathrm{d}^{k-1}}{\mathrm{d}\mathtt{h}^{k-1}} g(\mathtt{h})\bigg|_{\mathtt{h}=0} = \frac{1}{n}\,\frac{\mathrm{d}^{k}}{\mathrm{d}\mathtt{h}^{k}} H(X|Y(\mathtt{h}))\bigg|_{\mathtt{h}=0}.$$

In order to evaluate the last derivative, we can first assume that the i-th bit is transmitted through a channel BMS$(\mathtt{h}_i)$. Next we take partial derivatives with respect to k of the entropies $\{\mathtt{h}_i\}$. Finally we set $\mathtt{h}_i = 0$ for all bits i. We get therefore (neglecting the factor $1/n$):

$$\sum_{i_1 \ldots i_k} \frac{\partial^k}{\partial \mathtt{h}_{i_1} \cdots \partial \mathtt{h}_{i_k}} H(X|Y)\bigg|_{\mathtt{h}_i=0}.$$

Of course h_i can be set to 0 right at the beginning for all the bits that are not differentiated over. This is equivalent to passing the exact bits X_i. We get the expression

$$\sum_{i_1 \ldots i_k} \frac{\partial^k}{\partial \mathtt{h}_{i_1} \cdots \partial \mathtt{h}_{i_k}} H(X|Y_{i_1}(\mathtt{h}_{i_1}) \ldots Y_{i_k}(\mathtt{h}_{i_k}), X_{\sim i_1 \ldots i_k})$$

to be evaluated at $\mathtt{h}_{i_1} = \cdots = \mathtt{h}_{i_k} = 0$. If the code has minimum distance larger than k, then any $n-k$ bits determine the whole codeword and $H(X|Y_{i_1}(\mathtt{h}_{i_1}) \ldots Y_{i_k}(\mathtt{h}_{i_k}), X_{\sim i_1 \ldots i_k}) = 0$. This finishes the proof. ∎

So far we have used the compact notation $g(\mathtt{h})$ for the GEXIT function. In some circumstance it is more convenient to use a notation that makes the dependence of the functional on the involved densities more explicit.

Definition 4 (Alternative Notation for GEXIT Functional): Consider a binary linear code and transmission over a smooth family of BMS channels characterized by the associated family of L-densities $\{\mathsf{c}_\epsilon\}_\epsilon$. Let $\{\mathsf{a}_\epsilon\}_\epsilon$ denote the associated family of average extrinsic MAP densities (which we assume smooth). Define

$$G(\mathsf{c}_\epsilon, \mathsf{a}_\epsilon) \triangleq \int_{-\infty}^{\infty} \mathsf{a}_\epsilon(z) l^{\mathsf{c}_\epsilon}(z)\mathrm{d}z,$$

where

$$l^{\mathsf{c}_\epsilon}(z) = \frac{\int_{-\infty}^{\infty} \frac{\mathrm{d}\mathsf{c}_\epsilon(w)}{\mathrm{d}\epsilon} \log(1+e^{-z-w})\mathrm{d}w}{\int_{-\infty}^{\infty} \frac{\mathrm{d}\mathsf{c}_\epsilon(w)}{\mathrm{d}\epsilon} \log(1+e^{-w})\mathrm{d}w}.$$

Lemma 8 (GEXIT and Dual GEXIT Function): Consider a binary code C and transmission over a complete and smooth family of BMS channels characterized by the associated family of L-densities $\{\mathsf{c}_\epsilon\}_\epsilon$. Let $\{\mathsf{a}_\epsilon\}_\epsilon$ denote the corresponding family of (average) extrinsic MAP densities. Then the standard GEXIT curve is given in parametric form by $\{H(\mathsf{c}_\epsilon), G(\mathsf{c}_\epsilon, \mathsf{a}_\epsilon)\}$. The *dual* GEXIT curve is defined by $\{G(\mathsf{a}_\epsilon, \mathsf{c}_\epsilon), H(\mathsf{a}_\epsilon)\}$. Both, standard and dual GEXIT curve have an area equal to $r(C)$, the rate of the code.

Discussion: Note that both curves are "comparable" in that the first component measures the channel c and the second argument measure the MAP density a. The difference between the two lies in the choice of measure which is applied to each component.

Proof: The statement that $\{H(\mathsf{c}_\epsilon), G(\mathsf{c}_\epsilon, \mathsf{a}_\epsilon)\}$ represents the standard GEXIT function follows by unwinding the corresponding definitions. The only statement that requires a proof is the one concerning the area under the "dual GEXIT" curve. We proceed as follows: Consider the entropy $H(\mathsf{c}_\epsilon \star \mathsf{a}_\epsilon)$. We have

$$\begin{aligned} H(\mathsf{c}_\epsilon \star \mathsf{a}_\epsilon) &= \int_{-\infty}^{\infty} \Big(\int_{-\infty}^{\infty} \mathsf{c}_\epsilon(w)\mathsf{a}_\epsilon(v-w)\mathrm{d}w \Big) \log(1+e^{-v})\mathrm{d}v \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathsf{c}_\epsilon(w)\mathsf{a}_\epsilon(z) \log(1+e^{-w-z})\mathrm{d}w\mathrm{d}z. \end{aligned}$$

Consider now $\frac{\mathrm{d}H(\mathsf{c}_\epsilon \star \mathsf{a}_\epsilon)}{\mathrm{d}\epsilon}$. Using the previous representation we get

$$\begin{aligned} \frac{\mathrm{d}H(\mathsf{c}_\epsilon \star \mathsf{a}_\epsilon)}{\mathrm{d}\epsilon} &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{\mathrm{d}\mathsf{c}_\epsilon(w)}{\mathrm{d}\epsilon}\mathsf{a}_\epsilon(z) \log(1+e^{-w-z})\mathrm{d}w\mathrm{d}z + \\ &\quad \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathsf{c}_\epsilon(w)\frac{\mathrm{d}\mathsf{a}_\epsilon(z)}{\mathrm{d}\epsilon} \log(1+e^{-w-z})\mathrm{d}w\mathrm{d}z. \end{aligned}$$

The first expression can be identified with the standard GEXIT curve except that it is parameterized by a generic parameter ϵ. The second expression is essentially the same, but the roles of the two densities are exchanged. Integrate now this relationship over the whole range of ϵ and assume that this range goes from "perfect" (channel) to "useless". The integral on the left clearly equals 1. To perform the integrals on the right, reparameterize the first expression with respect to $\mathtt{h} \triangleq \int_{\infty}^{\infty} \mathsf{c}_\epsilon(w)\log(1+e^{-w})\mathrm{d}w$ so that the integral is equal to the area under the standard GEXIT curve given by $\{H(\mathsf{c}_\epsilon), G(\mathsf{c}_\epsilon, \mathsf{a}_\epsilon)\}$. In the same manner, reparameterize the second expression by $\mathtt{h} \triangleq \int_{\infty}^{\infty} \mathsf{a}_\epsilon(w)\log(1+e^{-w})\mathrm{d}w$. Therefore the value of second expression is equal the area under the curve given by $\{H(\mathsf{a}_\epsilon), G(\mathsf{a}_\epsilon, \mathsf{c}_\epsilon)\}$. Since the sum of the two areas equals one and the area under the standard GEXIT curve equals $r(C)$, it follows that the area under the second curve equals $1-r(C)$. Finally, note that if we consider the inverse of the second curve by exchanging the two coordinates, i.e., if we consider the curve $\{G(\mathsf{a}_\epsilon, \mathsf{c}_\epsilon), H(\mathsf{a}_\epsilon)\}$, then the area under this curve is equal to $1-(1-r(C)) = r(C)$, as claimed. ∎

Example 15 (GEXIT Versus Dual GEXIT): Fig. 6 shows the standard GEXIT function and the dual GEXIT function for the $[5,4,2]$ code and transmission over the BSC. Although the two curves have quite distinct shapes, the area under the two curves is the same.

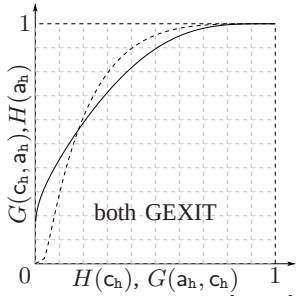

Fig. 6. Standard and dual GEXIT function of $[5,4,2]$ code and transmission over the BSC.

V. Ensembles: Concentration and Asymptotic Setting

For simple codes, like, e.g., single parity-check codes or repetition codes, h and g are relatively easy to compute. In general though it is not a trivial matter to determine the density of Φ_i required for the calculation. What we *can* typically compute are the extrinsic estimates if we use the BP decoder instead of the MAP decoder. It is therefore natural to look at the equivalent of EXIT and GEXIT functions if we substitute the extrinsic MAP estimates by their equivalent extrinsic BP estimates. Although most of the subsequent definitions and statements can be as easily derived for EXIT as for GEXIT functions, we focus on the latter. After all, these are the natural objects to study as suggested by the GAT.

Definition 5 (g^{BP} for Linear Codes and BMS Channels): Let X be chosen uniformly at random from a proper binary linear code. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i through the smooth family $\{\mathrm{BMS}(\mathtt{h}_i)\}_{\mathtt{h}_i}$, $\mathtt{h}_i \in [0,1]$. Assume that all individual channels are parameterized in a smooth way by a common parameter ϵ, i.e., $\mathtt{h}_i = \mathtt{h}_i(\epsilon)$, $i \in [n]$. Let $\Phi_i^{\text{BP},\ell}$ denote the extrinsic estimate of the i^{th} bit at the ℓ^{th} round of BP decoding, assuming an arbitrary but fixed representation of the code by a Tanner graph as well as an arbitrary but fixed schedule of the decoder. Then the BP GEXIT function is defined as

$$g_i^{\text{BP},\ell}(\epsilon) \triangleq \frac{\partial H(X_i|\Phi_i^{\text{BP},\ell}, Y_i)}{\partial \mathtt{h}_i}\frac{\mathrm{d}\mathtt{h}_i}{\mathrm{d}\epsilon}\Big|_\epsilon.$$

The following statement, which is a direct consequence of the previous definition and Lemma 4, confirms the intuitive fact that the BP GEXIT function (which is associated to the suboptimal BP decoder) is at least as large as the the GEXIT function itself, assuming only that the channel family is degraded.

Corollary 2 (GEXIT Versus BP GEXIT): Let X be chosen uniformly at random from a proper binary linear code. Let the channel from X to Y be memoryless, where Y_i is the result of passing X_i through a smooth and degraded family $\{\mathrm{BMS}(\mathtt{h}_i)\}_{\mathtt{h}_i}$, $\mathtt{h}_i \in [0,1]$. Assume that all individual channels are parameterized in a smooth (differentiable) way by a common parameter ϵ, i.e., $\mathtt{h}_i = \mathtt{h}_i(\epsilon)$, $i \in [n]$. Let $g_i(\epsilon)$ and $g_i^{\text{BP},\ell}(\epsilon)$ be as defined in Definitions 3 and 5. Then

$$g_i(\epsilon) \le g_i^{\text{BP},\ell}(\epsilon).$$

Definition 6 (Asymptotic BP EXIT and GEXIT Functions): Consider a dd pair (λ,ρ) and the corresponding sequence of ensembles $\mathrm{LDPC}(n,\lambda,\rho)$. Further consider a smooth and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Assume that all bits of X are sent through the channel $\mathrm{BMS}(\mathtt{h})$. For $\mathtt{G} \in \mathrm{LDPC}(n,\lambda,\rho)$ and $i \in [n]$, let $g_i(\mathtt{G},\epsilon)$ and $g_i^{\text{BP},\ell}(\mathtt{G},\epsilon)$ denote the i^{th} MAP and BP GEXIT function associated to code $\mathtt{G}$. By some abuse of notation, define the asymptotic (and average) quantities

$$g(\mathtt{h}) \triangleq \limsup_{n\to\infty} \mathbb{E}_{\mathtt{G}}\Big[\frac{1}{n}\sum_{i\in[n]} g_i(\mathtt{G},\mathtt{h})\Big],$$

$$g^{\text{BP},\ell}(\mathtt{h}) \triangleq \lim_{n\to\infty} \mathbb{E}_{\mathtt{G}}\Big[\frac{1}{n}\sum_{i\in[n]} g_i^{\text{BP},\ell}(\mathtt{G},\mathtt{h})\Big],$$

$$g^{\text{BP}}(\mathtt{h}) \triangleq \lim_{\ell\to\infty} g^{\text{BP},\ell}(\mathtt{h}).$$

For notational simplicity we suppress the dependence of the above quantities on the dd pair and the channel family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$.

In the above definitions we have taken the average of the individual curves over the ensemble. Let us now justify this approach by showing that the quantities are concentrated. The proof of the following statement, which asserts the concentration of the conditional entropy, can be found in [5].

Theorem 2 (Concentration of Conditional Entropy): Let $\mathtt{G}(n)$ be chosen uniformly at random from $\mathrm{LDPC}(n,\lambda,\rho)$. Assume that $\mathtt{G}(n)$ is used to transmit over a $\mathrm{BMS}(\mathtt{h})$ channel. By some abuse of notation, let $H_{\mathtt{G}(n)} = H_{\mathtt{G}(n)}(X\,|\,Y)$ be the associated conditional entropy. Then for any $\xi > 0$

$$\Pr\big\{|H_{\mathtt{G}(n)} - \mathbb{E}_{\mathtt{G}(n)}[H_{\mathtt{G}(n)}]| > n\xi\big\} \le 2\,\mathrm{e}^{-nB\xi^2},$$

where $B = 1/(2(\mathtt{r}_{\max}+1)^2(1-r))$ and $\mathtt{r}_{\max}$ is the maximal check-node degree.

Theorem 3 (Concentration of $g^{\text{BP},\ell}$): Consider the sequence of ensembles $\mathrm{LDPC}(n,\lambda,\rho)$, where (λ,ρ) is fixed and n tends to infinity. Then the limits $g^{\text{BP},\ell}(\mathtt{h}) = \lim_{n\to\infty} n^{-1}\mathbb{E}_{\mathtt{G}}[\sum_{i\in[n]} g_i^{\text{BP},\ell}(\mathtt{G},\mathtt{h})]$ and $g^{\text{BP}}(\mathtt{h}) = \lim_{\ell\to\infty} g^{\text{BP},\ell}(\mathtt{h})$ exist. Further, let $\mathtt{G}(n)$ be chosen uniformly at random from $\mathrm{LDPC}(n,\lambda,\rho)$. Assume that $\mathtt{G}(n)$ is used to transmit over a $\mathrm{BMS}(\mathtt{h})$ channel. Then, for all $\xi > 0$, there exists $\alpha_\xi > 0$, such that, for n large enough

$$\Pr\left\{\left|g^{\text{BP},\ell}(\mathtt{G}(n),\mathtt{h}) - g^{\text{BP},\ell}(\mathtt{h})\right| > n\xi\right\} \le \mathrm{e}^{-\alpha_\xi n}. \quad (13)$$

Proof: Note that for a fixed iteration number ℓ, the distribution of Φ_i^{BP} (with i a uniformly random node), assuming that the all-one codeword was sent, converges (at a speed of $1/n$) to the corresponding distribution of density evolution, denote it by $\mathtt{a}_\ell$. The result now follows by noting that $g^{\text{BP},\ell}$ is the result of applying a bounded linear operator to this distribution $\mathtt{a}_\ell$. The proof of concentration is almost verbatimly the same as the proof in [11], which shows the concentration of the probability of error under BP decoding, or the proof in [5], which relates to the concentration of the BP EXIT function. We will therefore skip the details. ∎

Theorem 4 (Concentration of g): Let $\mathtt{G}$ be chosen uniformly at random from $\mathrm{LDPC}(n,\lambda,\rho)$ and consider the smooth and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$, $\mathtt{h}\in[0,1]$. Assume that $\mathtt{G}$ is used to transmit over the $\mathrm{BMS}(\mathtt{h})$ channel. Let $H_{\mathtt{G}(n)} = H_{\mathtt{G}(n)}(X\,|\,Y)$ be the associated conditional entropy, $g(\mathtt{G}(n),\mathtt{h})$ the corresponding MAP GEXIT function, and $g_n(\mathtt{h}) = \mathbb{E}\, g(\mathtt{G}(n),\mathtt{h})$. Let $J\subseteq[0,1]$ be an interval on which $\lim_{n\to\infty}\frac{1}{n}\mathbb{E}\left[H_{\mathtt{G}(n)}\right]$ exists and is differentiable with respect to $\mathtt{h}$. Then, for any $\epsilon\in J$ and $\xi>0$ there exist an $\alpha_\xi>0$ such that, for n large enough

$$\Pr\left\{|g(\mathtt{G}(n),\mathtt{h}) - g_n(\mathtt{h})| > n\xi\right\} \le \mathrm{e}^{-n\alpha_\xi}.$$

Furthermore, if $\lim_{n\to\infty}\frac{1}{n}\mathbb{E}\left[H_{\mathtt{G}(n)}\right]$ is twice differentiable with respect to $\mathtt{h}\in J$, there exists a strictly positive constant A such that $\alpha_\xi > A\xi^4$.
The proof of this statement can be found in [5].

Let us summarize. We have seen that all the quantities which we introduced in Definition 6 are concentrated and that the BP quantities $g^{\text{BP},\ell}$ and g^{BP} exist. Unfortunately, we had to use $\limsup$ for the definition of g since to prove the existence of the limit seems to be difficult. As discussed in [5], even in the case of transmission over the BEC the existence of the corresponding limit is not known in general but only follows from the explicit construction of the Maxwell decoder in all those cases where the Maxwell construction can be shown to result in MAP performance.

Note that $g^{\text{BP},\ell}$ and g^{BP} have again a convenient representation in terms of the asymptotic BP densities. More precisely, we have

$$g^{\text{BP},\ell}(\mathtt{h}) = \int_{-\infty}^{\infty} \mathtt{a}^{\text{BP},\ell}(z) l^{\mathtt{c}_{\text{BMS}(\mathtt{h})}}(z)\,\mathrm{d}z,$$
$$g^{\text{BP}}(\mathtt{h}) = \int_{-\infty}^{\infty} \mathtt{a}^{\text{BP}}(z) l^{\mathtt{c}_{\text{BMS}(\mathtt{h})}}(z)\,\mathrm{d}z,$$

where $\mathtt{a}^{\text{BP},\ell}$ is the limiting density of $\Phi_i^{\text{BP},\ell}$ (with i a uniformly random node) under the all-one codeword assumption as n tends to infinity associated to the dd pair (λ,ρ). This density can easily be computed by density evolution. In a similar manner, $\mathtt{a}^{\text{BP}}$ is the corresponding fixed-point density of density evolution.

In Fig. 7 we plot the BP GEXIT function g^{BP} for a few regular LDPC ensembles and we compare them with the corresponding BP EXIT functions, which we denote by h^{BP}. We see that the curves are quite similar.

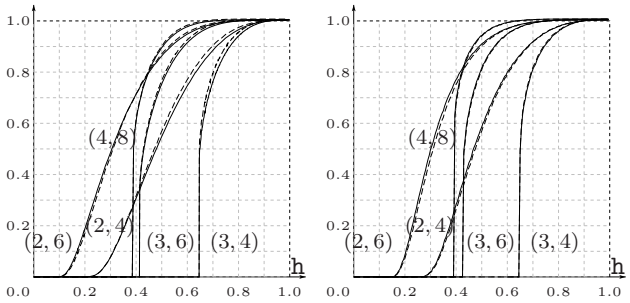

Fig. 7. BP GEXIT (solid curves) versus BP EXIT (dashed curves) for several regular LDPC ensembles for the BSC (left picture) and the BAWGNC (right picture).

Lemma 9 ($g \le g^{\text{BP}}$): Consider a dd pair (λ,ρ) and transmission over the smooth and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Let $g(\mathtt{h})$ and $g^{\text{BP}}(\mathtt{h})$ denote respectively the corresponding asymptotic MAP and BP GEXIT functions as defined in Definition 6 when the code is chosen uniformly at random from the ensemble $\mathrm{LDPC}(n,\lambda,\rho)$. Then

$$g(\mathtt{h}) \le g^{\text{BP}}(\mathtt{h}).$$

Proof: Using Corollary 2, we know that for any $\mathtt{G}\in\mathrm{LDPC}(n,\lambda,\rho)$ and $\ell\in\mathbb{N}$

$$g_{\mathtt{G}}(\epsilon) \le g_{\mathtt{G}}^{\text{BP},\ell}(\epsilon).$$

If we take first the expectation over the elements of the ensemble, then the $\limsup$ on both sides with respect to n, and finally the limit $\ell\to\infty$, we get the desired result. ∎

VI. An Upper Bound on the MAP Threshold

One important consequence of the area theorem is that it gives rise to an easy to compute upper bound on the threshold of MAP decoding.

Definition 7 (MAP Threshold): Consider a dd pair (λ,ρ) and a smooth and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. The *threshold* $\mathtt{h}^{\text{MAP}}$ is *defined* as

$$\mathtt{h}^{\text{MAP}} \triangleq \min\{\mathtt{h}\in[0,1] : \liminf_{n\to\infty} \mathbb{E}_{\mathtt{G}}[H(X\,|\,Y(\mathtt{h}))]/n > 0\}.$$

Discussion: Let us consider the operational meaning of the above definition. Let $\mathtt{h} < \mathtt{h}^{\text{MAP}}$. Then by definition of the threshold, there exists a sequence of blocklengths $n_1, n_2, n_3, \cdots$, so that the normalized (divided by the blocklength n) *average* conditional entropy converges to zero. By Theorem 2 it follows that most of the codes in the corresponding ensembles have a normalized conditional entropy less

than any fixed constant. For sufficiently large blocklengths, a conditional entropy which grows sublinearly implies that the receiver can limit the set of hypothesis to a subexponential list which with high probability contains the correct codeword. Therefore, in this sense reliable communication is possible.

On the other hand, assume that $\mathtt{h} > \mathtt{h}^{\text{MAP}}$. In this case the normalized conditional entropy stays bounded away from zero by a strictly positive constant for all sufficiently large blocklengths. By Theorem 2 this is not only true for the average over the ensemble but for most elements from the ensemble. It follows that with most elements from the ensemble reliable communication is not possible.

Theorem 5 (Upper Bound on MAP Threshold): Consider a dd pair (λ, ρ) whose asymptotic rate converges to the design rate $r(\lambda, \rho)$, see [5, Lemma 7]. Assume further that transmission takes place over a smooth and degraded family $\{\text{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Let $g^{\text{BP}}(\mathtt{h})$ denote the associated BP GEXIT function. Then

$$\liminf_{n\to\infty} \mathbb{E}_{\mathtt{G}}[H(X \,|\, Y(\mathtt{h}))]/n \geq r(\lambda,\rho) - \int_{\mathtt{h}}^{1} g^{\text{BP}}(\mathtt{h}')\, \mathrm{d}\mathtt{h}'\,. \tag{14}$$

Furthermore, if $\overline{\mathtt{h}}$ denotes the largest positive number so that

$$\int_{\overline{\mathtt{h}}}^{1} g^{\text{BP}}(\mathtt{h})\, \mathrm{d}\mathtt{h} = r(\lambda,\rho),$$

then $\mathtt{h}^{\text{MAP}} \leq \overline{\mathtt{h}}$, where $\mathtt{h}^{\text{MAP}}$ denotes the MAP threshold.

Proof: Let $\mathtt{G}$ be chosen uniformly at random from the ensemble $\text{LDPC}(n, \lambda, \rho)$. By the GAT

$$\begin{aligned} r(\lambda,\rho) - \liminf_{n\to\infty} \mathbb{E}_{\mathtt{G}}[H(X \,|\, Y(\mathtt{h}))]/n = \\ = \limsup_{n\to\infty} \frac{1}{n}\, \mathbb{E}_{\mathtt{G}}[H(X \,|\, Y(1)) - H(X \,|\, Y(\mathtt{h}))] = \\ = \limsup_{n\to\infty} \mathbb{E}_{\mathtt{G}}\Big[\int_{\mathtt{h}}^{1} g(\mathtt{G}, \mathtt{h}')\, \mathrm{d}\mathtt{h}'\Big]. \end{aligned}$$

We can exchange the expectation and the integral by Fubini's theorem: in fact $g(\mathtt{G}, \mathtt{h}')$ is measurable and $g(\mathtt{G}, \mathtt{h}') \in [0,1]$. We can furthermore exchange the limit and the integral by the Fatou-Lebesgue lemma. We get

$$\liminf_{n\to\infty} \mathbb{E}_{\mathtt{G}}[H(X \,|\, Y(\mathtt{h}))]/n \geq r(\lambda,\rho) - \int_{\mathtt{h}}^{1} g(\mathtt{h}')\, \mathrm{d}\mathtt{h}'\,.$$

Equation (14) is proved by applying Lemma 9.

The upper bound on the MAP threshold follows from the observation that the r.h.s. of Eq. (14) is non-decreasing in h. Therefore $\limsup_{n\to\infty} \mathbb{E}_{\mathtt{G}}[H(X \,|\, Y(\mathtt{h}))]/n$ is bounded away from 0 for any $\mathtt{h} > \overline{\mathtt{h}}$ and the thesis follows from the definition of $\mathtt{h}^{\text{MAP}}$. ∎

Example 16: The following table presents the upper bounds on the MAP threshold for transmission over the BAWGNC($\mathtt{h}$) as derived from Theorem 5 for a few regular ensembles: $\lambda(x) = x^{\mathtt{l}-1}$, $\rho(x) = x^{\mathtt{r}-1}$. The same threshold were first computed using the (non-rigorous) replica method from statistical physics [27]. In [28], they were shown to be upper bounds for $\mathtt{r}$ even, using an interpolation technique. The present proof applies also to the case of odd $\mathtt{r}$. It can be proved that the three characterizations of the threshold are indeed equivalent, i.e., they give *exactly* the same value.

$\mathtt{l}$	$\mathtt{r}$	$\mathtt{h}^{\text{BP}}$	$\overline{\mathtt{h}}$	$\overline{\mathtt{h}}$([29], [30])	$\mathtt{h}^{\text{Sh}}$
3	4	0.6507(5)	0.7417(1)	0.743231	3/4
3	5	0.5113(5)	0.5800(3)	0.583578	3/5
3	6	0.4160(5)	0.4721(5)	0.476728	1/2
4	6	0.5203(5)	0.6636(2)	0.663679	1/3

Also shown is the result of the information theoretic upper bound given in [29], which in turn is an improved version of the bound developed in [30]. For the specific case of transmission over the BSC and regular codes it is given by $h_2(\overline{\epsilon})$, where $\overline{\epsilon}$ is the unique positive root of the equation $\mathtt{r} h_2(\epsilon) = \mathtt{l} h_2((1-(1-2\epsilon)^{\mathtt{r}})/2)$.

VII. The Extended BP GEXIT Curve

A. Extended BP GEXIT Curve

As discussed in detail in [5] for the case of transmission over the BEC, the fundamental relationship which appears in the limit of large blocklengths between the MAP and the BP decoder is best described in terms of the *extended* EXIT curve. For the BEC this is the curve with parametric description $\Big(\frac{\mathtt{x}}{\lambda(1-\rho(1-\mathtt{x}))}, \Lambda(1-\rho(1-\mathtt{x}))\Big)$, where $\mathtt{x}$ takes values in the subset $J \subseteq [0,1]$ such that $\mathtt{x} \leq \lambda(1-\rho(1-\mathtt{x}))$ (J is in fact the union of a finite number of intervals). Note that the families $\{\mathsf{f}_{\mathtt{x}}\}_{\mathtt{x}} \triangleq \{\text{BEC}(\mathtt{x})\}_{\mathtt{x}}$ and $\{\mathsf{c}_{\mathtt{x}}\}_{\mathtt{x}} \triangleq \{\text{BEC}(\frac{\mathtt{x}}{\lambda(1-\rho(1-\mathtt{x}))}\}_{\mathtt{x}}$, $\mathtt{x} \in J$, have the following property: For each $\mathtt{x} \in J$, $\mathsf{f}_{\mathtt{x}}$ constitutes a fixed-point density (of density evolution) for the channel $\mathsf{c}_{\mathtt{x}}$. Furthermore both channel families are *smooth* and satisfy $H(\mathsf{f}_{\mathtt{x}}) = \mathtt{x}$. Finally if $J = [0,1]$ (a necessary condition for this to happen is $\lambda'(0)\rho'(1) \geq 1$) the families are said to be *complete*.

Definition 8 (Complete Fixed-Point Family, g^{EBP} and g^{BP}): Consider a degree distribution pair (λ, ρ). We say that the families $\{\mathsf{f}_{\mathtt{x}}\}_{\mathtt{x}}$ and $\{\mathsf{c}_{\mathtt{x}}\}_{\mathtt{x}}$, $\mathtt{x} \in [0,1]$, form a *complete fixed-point family* for (λ, ρ) if

(i) there exists a complete and degraded family $\{\text{BMS}(\mathtt{h})\}_{\mathtt{h}}$ such that for each $\mathtt{x} \in [0,1]$, $\mathsf{c}_{\mathtt{x}} \in \{\text{BMS}(\mathtt{h})\}_{\mathtt{h}}$
(ii) for each $\mathtt{x} \in [0,1]$, $\mathsf{f}_{\mathtt{x}}$ is a fixed-point density with respect to the degree distribution (λ, ρ) and the channel $\mathsf{c}_{\mathtt{x}}$; this means that for each $\mathtt{x} \in [0,1]$, $\mathsf{f}_{\mathtt{x}} = \mathsf{c}_{\mathtt{x}} \star \lambda(\rho(\mathsf{f}_x))$
(iii) $\{\mathsf{f}_{\mathtt{x}}\}_{\mathtt{x}}$ and $\{\mathsf{c}_{\mathtt{x}}\}_{\mathtt{x}}$ are smooth with respect to $\mathtt{x}$
(iv) $H(\mathsf{f}_{\mathtt{x}}) = \mathtt{x}$

Let $\mathsf{a}_{\mathtt{x}}(y) \triangleq \Lambda(\rho(\mathsf{f}_{\mathtt{x}}))$. The *extended* BP (EBP) GEXIT curve, call it $g^{\text{EBP}}(\mathtt{x})$, is then given in parametric form by $(H(\mathtt{x}), g^{\text{EBP}}(\mathtt{x}))$, where

$$g^{\text{EBP}}(\mathtt{x}) \triangleq \int_{-\infty}^{\infty} \mathsf{a}_{\mathtt{x}}(y) l^{\mathsf{c}_{\mathtt{x}}}(y)\, \mathrm{d}y.$$

Finally, the BP GEXIT curve, call it g^{BP}, is the "envelope" of the g^{EBP} curve.

Discussion: Contrary to our usual notation, we have used $\mathtt{x}$ to parameterize the channel families and the function $g^{\text{EBP}}(\mathtt{x})$ and we have assumed that $H(\mathsf{f}_{\mathtt{x}}) = \mathtt{x}$ (rather than $H(\mathsf{c}_{\mathtt{x}}) = \mathtt{x}$). This has the following reason: in general, the EBP GEXIT function is not a single-valued function of the *channel* entropy but it is a single-valued function of the *fixed-point* entropy (see Fig. 1). We prefer to use the parameter $\mathtt{x}$ instead of the usual parameter $\mathtt{h}$, to remind ourselves that the channel $\mathsf{c}_{\mathtt{x}}$ is the channel which belongs to the fixed-point density $\mathsf{f}_{\mathtt{x}}$ (and not

the channel $\mathtt{c}_{\mathtt{h}}$, which by our previous notational convention has entropy $\mathtt{h}$). *Complete* fixed-point families do not always exist. If, for instance, $\lambda_2 = 0$, then $\mathtt{x}$ cannot be chosen arbitrarily close to 0. This is easily seen for transmission over the BEC. In this case $\mathtt{x} \geq \underline{\mathtt{x}}$ with $\underline{\mathtt{x}}$ the smallest (non-vanishing) root of the equation $\lambda(1-\rho(1-\mathtt{x})) = \mathtt{x}$.

From the definition it is not immediately obvious that for a given degree distribution pair (λ, ρ) and a complete and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$, such a (complete or incomplete) fixed-point family always exists, or that it is unique. For the BEC we have an explicit formula for the family, but in the general case the existence is far from trivial. We will get back to this point in the next section.

One of the important applications of the EBP GEXIT curve is that it encodes very clearly the connection between MAP and BP decoding. As mentioned above, the BP GEXIT function is obtained as the 'envelope' of the EBP curve. More precisely, one has to choose, for each value of the channel entropy $\mathtt{h}$, the branch of the EBP curve whose GEXIT value is the largest. As pointed out in the introduction when discussing Fig. 1, a different single valued function can be obtained by applying the Maxwell construction, described in detail in [5], to the EBP GEXIT curve. Motivated by the GAT as well as by the BEC case, we formulate the following

Conjecture 1: The (MAP) GEXIT function $g(\mathtt{h})$ is obtained by applying the Maxwell construction to the extended BP GEXIT curve $(H(\mathtt{x}), g^{\mathrm{EBP}}(\mathtt{x}))$.

Let us consider a few typical examples. In each of the following cases the complete fixed-point family was computed by a *numerical* procedure, which will be explained in the next section.

Example 17 (LDPC(x, x^5) – BSC): Consider the dd pair $(\lambda, \rho) = (x, x^5)$ and the corresponding LDPC ensemble with design rate $r = 2/3$. We assume that transmission takes place over the family $\{\mathrm{BSC}(\epsilon)\}$. Recall that for this code the BP threshold is given by the stability condition. From Fig. 8 we see that, according to the numerical calculation, the EBP GEXIT curve is a monotone function. Assuming this is true, it follows that the EBP GEXIT is equal to the BP GEXIT curve for this example. For any value of the channel parameter a single fixed point density (apart from the 'delta at infinity') is found. Also: a single fixed point density exists for each value of the density entropy $\mathtt{x}$. The Maxwell construction is trivial in this case and yields a MAP GEXIT equal to the BP GEXIT curve.

Example 18 ((3,6) LDPC Ensemble – BSC): Consider the dd pair $(\lambda, \rho) = (x^2, x^5)$ and the corresponding LDPC ensemble with design rate $r = 1/2$. We assume that transmission takes place over the family $\{\mathrm{BSC}(\epsilon)\}$. Fig. 9 shows on the left the EBP GEXIT curve and the corresponding BP GEXIT curve, which has one jump. The picture on the right shows the conjectured MAP GEXIT curve according to the Maxwell construction. For this ensemble, we have $\mathtt{h}^{\mathrm{BP}} \approx 0.416$. The MAP threshold implied by the Maxwell construction coincides with the one of Theorem 5: $\overline{\mathtt{h}}^{\mathrm{MAP}} \approx 0.472$.

Example 19 (LDPC($2/5x + 3/5x^5, x^5$) – BSC): Consider the dd pair $(\lambda, \rho) = (2/5x + 3/5x^5, x^5)$ and the corresponding LDPC ensemble with design rate $r = 4/9$. We assume that transmission takes place over the family $\{\mathrm{BSC}(\epsilon)\}$. Fig. 10 shows on the left the EBP GEXIT curve and the corresponding BP GEXIT curve, which has one jump. The picture on the right shows the conjectured MAP GEXIT curve according to the Maxwell construction. The BP threshold is given by the stability condition. As a consequence of this and Conjecture 1, $\mathtt{h}^{\mathrm{BP}} = \mathtt{h}^{\mathrm{MAP}}$.

Example 20 (LDPC($\frac{3x+6x^2+11x^{17}}{20}, x^9$) – BSC): Consider the dd pair $(\frac{3x+6x^2+11x^{17}}{20}, x^9)$. We assume that transmission takes place over the family $\{\mathrm{BSC}(\epsilon)\}$. Fig. 11 shows on the left the EBP GEXIT curve and the corresponding BP GEXIT curve, which has two jumps. The picture on the right shows the conjectured MAP GEXIT curve according to the Maxwell construction: This curve has also 2 jumps.

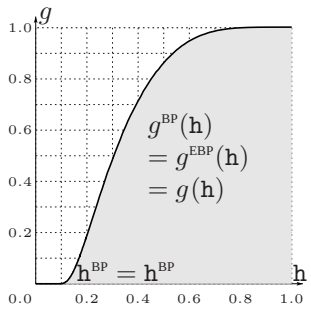

Fig. 8. EBP GEXIT curve for the cycle-code ensemble with dd pair (x, x^5). The EBP GEXIT curve, BP GEXIT curve and MAP GEXIT curve coincide.

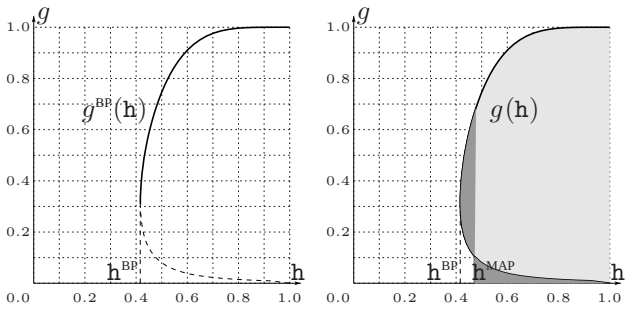

Fig. 9. EBP GEXIT curve for the $(3, 6)$ ensemble. Left: EBP GEXIT curve and corresponding BP GEXIT curve. Right: The conjectured MAP GEXIT curve according to the Maxwell construction.

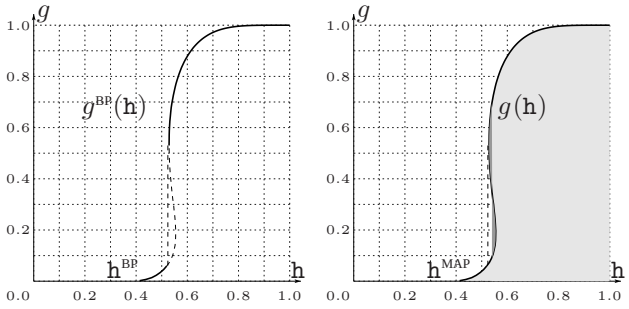

Fig. 10. EBP GEXIT curve for the $(\lambda, \rho) = (2/5x + 3/5x^5, x^5)$ ensemble. Left: EBP GEXIT curve and corresponding BP GEXIT curve. Right: The conjectured MAP GEXIT curve according to the Maxwell construction.

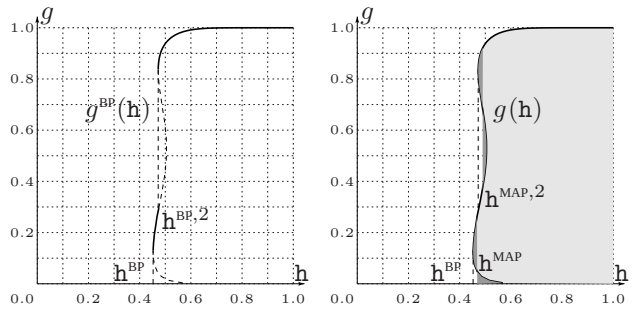

Fig. 11. EBP GEXIT curve for the dd pair $(\frac{3x+6x^2+11x^{17}}{20}, x^9)$. Left: EBP GEXIT curve and corresponding BP GEXIT curve. Right: The conjectured MAP GEXIT curve according to the Maxwell construction.

Example 21 ($(\frac{x+2x^2+2x^{13}}{5}, x^5)$ – BSC): Consider the dd pair $(\frac{x+2x^2+2x^{13}}{5}, x^5)$ and the corresponding LDPC ensemble. . We assume that transmission takes place over the family $\{\mathrm{BSC}(\epsilon)\}$. Fig. 12 shows on the left the EBP GEXIT curve and the corresponding BP GEXIT curve, which has two jumps. The picture on the right shows the conjectured MAP GEXIT curve according to the Maxwell construction. This example shows that a dd pair can have more BP jumps than MAP jumps.

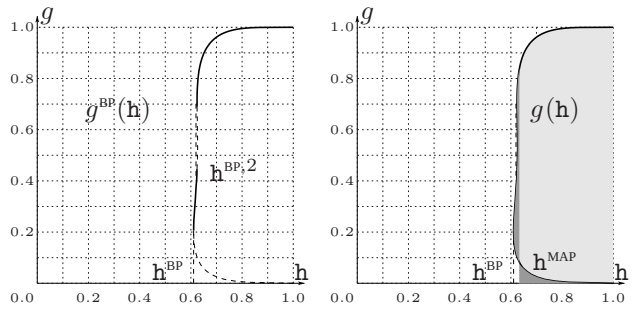

Fig. 12. EBP GEXIT curve for the dd pair $(\frac{x+2x^2+2x^{13}}{5}, x^5)$. Left: EBP GEXIT curve and corresponding BP GEXIT curve. Right: The conjectured MAP GEXIT curve according to the Maxwell construction.

VIII. How to Compute EBP GEXIT Curves: Basic Properties and Area Theorem

In the previous pages we presented examples of EBP GEXIT curves for several LDPC ensembles. In this section we explain how these curves have been computed and we derive some of their basic properties, including the EBP Area Theorem.

We start by noticing that ordinary density evolution cannot be applied to the present case because of two reasons. First, EBP curves include 'unstable branches'. We refer by such a term to branches along which the GEXIT curve is a decreasing function of the channel entropy. Such branches are expected to correspond to fixed point densities which are locally unstable under density evolution (whence the name). This expectation can be confirmed analytically for the BEC case, and numerically for a general BMS channel. As a consequence, these fixed points cannot be approximated by iterating density evolution with a generic initial condition.

The second problem is related to values of the channel parameter for which multiple locally stable fixed point densities coexist. This is the case for instance in the Examples 19 to 21 above. In this case different initial conditions are required to achieve each of these densities by density evolution. A systematic way for constructing all such initial conditions is however not available.

The crucial observation for overcoming both these problems consists in noticing that EBP GEXIT curves are naturally parameterized by the *entropy of the fixed point density*. More precisely, consider a smooth and degraded family $\{\mathrm{BMS}(\mathtt{h})\}$ and $\mathtt{x} \in [0,1]$. Then, we expect that there exists at most one value of the channel parameter $\mathtt{h} = \mathtt{h}(\mathtt{x})$ and one density $\mathsf{f}_\mathtt{x}$, such that $H(\mathsf{f}_\mathtt{x}) = \mathtt{x}$ and $(\mathsf{c}_\mathtt{x} \triangleq \mathrm{BMS}(\mathtt{h}(\mathtt{x})), \mathsf{f}_\mathtt{x})$ forms a fixed point pair.

This naturally suggests to run density evolution *at fixed density entropy*. Let us denote by $T_\mathtt{h}$ the ordinary density evolution operator at fixed channel $\mathrm{BMS}(\mathtt{h})$. Formally

$$T_\mathtt{h}(\mathsf{a}) \triangleq \mathsf{c} \star \lambda(\rho(\mathsf{a}))\,. \tag{15}$$

where c is the density associated to the channel $\mathrm{BMS}(\mathtt{h})$. For any $\mathtt{x} \in [0,1]$, we define the density evolution operator at fixed entropy $\mathtt{x}$, $R_\mathtt{x}$ as

$$R_\mathtt{x}(\mathsf{a}) \triangleq T_{\mathtt{h}(\mathtt{a},\mathtt{x})}(\mathsf{a}) \tag{16}$$

where $\mathtt{h}(\mathtt{a},\mathtt{x})$ is the solution of $H(T_\mathtt{h}(\mathsf{a})) = \mathtt{x}$. Whenever no such value of $\mathtt{h}$ exists, $R_\mathtt{x}(\mathsf{a})$ is left undefined. Since, for a given a, the family $T_\mathtt{h}(\mathsf{a})$ is ordered by physical degradation, $H(T_\mathtt{h}(\mathsf{a}))$ is a non decreasing function of $\mathtt{h}$. As a consequence the equation $H(T_\mathtt{h}(\mathsf{a})) = \mathtt{x}$ cannot have more than a single solution. Furthermore, by the smoothness of the channel family $\mathrm{BMS}(\mathtt{h})$, $H(T_\mathtt{h}(\mathsf{a}))$ is continuous. Notice that $H(T_0(\mathsf{a})) = 0$: if the channel is noiseless the output density at a variable nodes is noiseless as well. Therefore, a necessary and sufficient condition for a solution $\mathtt{h}(\mathtt{a},\mathtt{x})$ to exist (when the family $\{\mathrm{BMS}(\mathtt{h})\}_\mathtt{h}$ is complete) is that $H(T_1(\mathsf{a})) = H(\lambda(\rho(\mathsf{a}))) \geq \mathtt{x}$.

Any fixed point of the above transformation $R_\mathtt{x}$, i.e. any f such that $\mathsf{f} = R_\mathtt{x}(\mathsf{f})$, is also a fixed point of ordinary density evolution for the channel $\mathrm{BMS}(\mathtt{h})$ with $\mathtt{h} = \mathtt{h}(\mathsf{f},\mathtt{x})$, and corresponds to a point on the EBP GEXIT curve. Furthermore if a sequence of densities such that $\mathsf{a}_{\ell+1} = R_\mathtt{x}(\mathsf{a}_\ell)$ converges (weakly) to a density f, then f is a fixed point of $R_\mathtt{x}$, with entropy $\mathtt{x}$.

This motivates the following numerical procedure which has been used to determine the GEXIT curves plotted in the previous section. (i) Set the initial condition $\mathsf{a}_0 = \mathrm{BMS}(\mathtt{x})$. (ii) For $\ell \geq 0$ compute $\mathsf{a}_{\ell+1} = R_\mathtt{x}(\mathsf{a}_\ell)$. In practice the convolutions are evaluated numerically either by sampling or, via Fourier transforms as in ordinary density evolution. Due to the monotonicity of $H(T_\mathtt{h}(\mathsf{a}_\ell))$ in $\mathtt{h}$, the value of $\mathtt{h}(\mathsf{a}_\ell,\mathtt{x})$ can be efficiently found by bisection. (iii) The current estimate of the GEXIT function is given by $(\mathtt{h}_\ell, g_\ell^{\mathrm{EBP}})$. Here $\mathtt{h}_\ell \triangleq \mathtt{h}(\mathsf{a}_\ell,\mathtt{x})$ is the current estimate of the channel entropy, and

$$g_\ell^{\mathrm{EBP}} \triangleq \int_{-\infty}^{\infty} \mathsf{b}_\ell(y)\, l^{\mathrm{BMS}(\mathtt{h}_\ell)}(y)\, \mathrm{d}y. \tag{17}$$

with $\mathsf{b}_\ell \triangleq \Lambda(\rho(\mathsf{a}_\ell))$. (iv) Halt when some convergence criterion is met and return the current estimate $(\mathtt{h}_\ell, g_\ell^{\mathrm{EBP}})$. In

practice one can require that (a properly defined) distance between a_ℓ and $\mathsf{a}_{\ell+1}$ becomes smaller than a threshold.

In all the examples discussed in the previous section, we found that this procedure converges rapidly, and that the limit point is (within numerical precision) independent of the initial condition a_0. Proving these statements seems a challenging task (notice that unlike in ordinary density evolution, the sequence $\{\mathsf{a}_\ell\}$ is in general not ordered by physical degradation). However it is easy to show that, if $\mathtt{x}$ is such that $R_{\mathtt{x}}$ is 'well defined', then this procedure has at least one fixed point.

Theorem 6: Let (λ, ρ) be a dd pair , $\mathtt{x} \in [0,1]$, and $R_{\mathtt{x}}$ the corresponding density evolution operator at fixed density entropy defined as above, for the smooth, complete and degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. If $H(\lambda(\rho(\mathsf{a}))) \geq \mathtt{x}$ for any density a with $H(\mathsf{a}) = \mathtt{x}$, then there exists at least one density f such that $R_{\mathtt{x}}(\mathsf{f}) = \mathsf{f}$. Equivalently, $H(\mathsf{f}) = \mathtt{x}$ and there exists $\mathtt{h} \in [0,1]$ such that f is a fixed point of density evolution for the channel $\mathrm{BMS}(\mathtt{h})$.

Proof: Consider the space $\mathsf{S}_{\mathtt{x}}$ of L-densities a such that $H(\mathsf{a}) = \mathtt{x}$. Any element in $\mathsf{S}_{\mathtt{x}}$ is a probability measure on the completed real line, satisfying the symmetry condition (formally $\mathsf{a}(-x) = e^{-x}\mathsf{a}(x)$). Vice versa, any such probability measure (to be denoted formally by its 'density' a) with $\mathbb{E}[\log(1+e^{-x})] = \mathtt{x}$) corresponds to a unique element of $\mathsf{S}_{\mathtt{x}}$. Notice that the completed linear line $\mathbb{R}_\infty$ is a compact metric space (we can for instance identify it with $[-1,1]$ through the mapping $x \mapsto \tanh(x/2)$ and use the euclidean metric on $[-1,1]$). Therefore, the space of probability measure on $\mathbb{R}_\infty$ is sub-sequentially compact under the weak topology by Prohorov's theorem [31]. Both the symmetry condition and $H(\mathsf{a}) = \mathtt{x}$ are closed under the same topology, and therefore $\mathsf{S}_{\mathtt{x}}$ is compact as well.

Let BL be the space of bounded Lipshitz function on $\mathbb{R}_\infty$ (as above, we identify $\mathbb{R}_\infty$ with $[-1,1]$ and consider the Lipschitz condition with respect to the induced distance) with the corresponding norm $||\cdot||_{\mathsf{BL}}$. The space of probability measures on $\mathbb{R}_\infty$ can be viewed as a convex subset of the dual space BL^*, and the topology induced by the dual norm $||\cdot||^*_{\mathsf{BL}}$ coincides with the weak topology (cf. [31, Chapter III, §7]). As a consequence $\mathsf{S}_{\mathtt{x}}$ is a compact convex subspace of a normed linear space.

By hypothesis the mapping $\mathsf{a} \mapsto R_{\mathtt{x}}(\mathsf{a})$, is well defined for any $\mathsf{a} \in \mathsf{S}_{\mathtt{x}}$, and maps $\mathsf{S}_{\mathtt{x}}$ into itself. Furthermore, it is easily seen to be continuous with respect to the weak topology. This is a consequence of the Lipschitz continuity of the functions $(x_1, \dots, x_{\mathtt{l}}) \to (x_1 + \cdots + x_{\mathtt{l}})$ and $(x_1, \dots, x_{\mathtt{r}-1}) \to 2\,\mathrm{atanh}(\tanh(x_1/2)\cdots\tanh(x_{\mathtt{r}-1}/2))$. Therefore $R_{\mathtt{x}}$ is compact and, by Schauder's fixed point theorem (cf. [32], Chapter 4) it has at least one fixed point. ∎

Notice that the above procedure, as well as Theorem 6, holds unchanged if the entropy functional $H(\,\cdot\,)$ is substituted by any continuous linear functional which preserves physical degradation.

In checking the hypothesis of Theorem 6, as well as in applications, it is important to prove bounds on the entropy of fixed point pairs (f, c). We start by recalling upper and lower bounds on the entropy of $T_{\mathtt{h}}(\mathsf{a})$ which follows straightforwardly from [23]–[25], [33].

Lemma 10 (Lower Bound): Consider a dd pair (λ, ρ) and transmission over the channel $\mathrm{BMS}(\mathtt{h})$. Let

$$\underline{l}(\mathtt{x}) \triangleq \lambda(\mathtt{x}), \qquad \underline{r}(\mathtt{x}) \triangleq \sum_i \rho_i h_2\Big(\frac{1-(1-2\epsilon(\mathtt{x}))^{i-1}}{2}\Big),$$

where $\epsilon(\mathtt{x}) \triangleq h_2^{-1}(\mathtt{x})$. If a is an L-density with $H(\mathsf{a}) = \mathtt{x}$, then

$$H(T_{\mathtt{h}}(\mathsf{a})) \geq \mathtt{h}\,\underline{l}(\underline{r}(\mathtt{x}))\,.$$

Proof: Following Refs. [23]–[25], [33], for fixed $H(\mathsf{a})$ and $H(\mathsf{b})$, $\mathsf{a} \star \mathsf{b}$ has minimum entropy if a and b are the densities corresponding to a BEC. On the other hand, for the convolution at a parity-check node the minimum is achieved when the input densities correspond to a BSC. The lemma follows by applying these bounds to random variable and check nodes with degree distributions given by λ and ρ. ∎

This result can be used to check the hypotheses of Theorem 6. We deduce that, if $\underline{l}(\underline{r}(\mathtt{x})) \geq \mathtt{x}$ for some $\mathtt{x} \in [0,1]$, then there exists a fixed point pair (f, c) with $H(\mathsf{f}) = \mathtt{x}$ and $\mathsf{c} = \mathrm{BMS}(\mathtt{h})$ for some $\mathtt{h}$. For instance, for cycle codes (i.e., for $\lambda(x) = x$) this implies that such a fixed point pair (f, c) exists for any $H(\mathsf{f}) = \mathtt{x} \in [0,1]$.

Lemma 11 (Upper Bound): Consider a dd pair (λ, ρ) and transmission over the channel $\mathrm{BMS}(\mathtt{h})$. Let

$$\overline{l}(\mathtt{h}, \mathtt{x}) \triangleq \sum_i \lambda_i f_{i-1}(\mathtt{h}, \mathtt{x})\,, \qquad \overline{r}(\mathtt{x}) \triangleq \quad 1 - \rho(1-\mathtt{x})$$

where

$$f_i(\mathtt{h}, \mathtt{x}) \triangleq \sum_{k \in \{\pm 1\}} \sum_{j=0}^{i} \binom{i}{j} (1-\epsilon(\mathtt{x}))^j \epsilon(\mathtt{x})^{i-j} a_k(\mathtt{h}) \cdot \log_2\Big(1 + \frac{\epsilon(\mathtt{x})^{2j-i} a_{-k}(\mathtt{h})}{(1-\epsilon(\mathtt{x}))^{2j-i} a_k(\mathtt{h})}\Big)\,,$$

$a_{+1}(\mathtt{h}) \triangleq 1 - \epsilon(\mathtt{h})$, $a_{-1}(\mathtt{h}) \triangleq \epsilon(\mathtt{h})$, and $\epsilon(\mathtt{h}) \triangleq h_2^{-1}(\mathtt{h})$ as above. If a is an L-density with $H(\mathsf{a}) = \mathtt{x}$, then

$$H(T_{\mathtt{h}}(\mathsf{a})) \leq \overline{l}(\mathtt{h}, \overline{r}(\mathtt{x}))\,.$$

Proof: Apply the upper bounds of [23]–[25], [33] (simply interchange BEC and BSC). ∎

Theorem 7 (Bounds on EXIT Function): Consider a dd pair (λ, ρ) and transmission over the degraded family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$. Define the functions

$$\underline{L}(\mathtt{x}) \triangleq \Lambda(\mathtt{x})\,, \qquad \overline{L}(\mathtt{x}) \triangleq \sum_i \Lambda_i f_i(1, \mathtt{x}),$$

and $f(\mathtt{x}, \mathtt{x}') \triangleq \max\{\mathtt{h} : \overline{l}(\mathtt{h}, \mathtt{x}') = \mathtt{x}\}$ (with the convention $f(\mathtt{x}, \mathtt{x}') = 0$, if the set is empty). Let f denote any fixed point of density evolution, i.e., $\mathsf{f} = T_{\mathtt{h}}(\mathsf{f})$. If $H(\mathsf{f}) = \mathtt{x}$ then

$$f(\mathtt{x}, \overline{r}(\mathtt{x})) \leq \mathtt{h} \leq \mathtt{x}/\underline{l}(\underline{r}(\mathtt{x})),$$
$$\underline{L}(\underline{r}(\mathtt{x})) \leq h^{\text{EBP}} \leq \overline{L}(\overline{r}(\mathtt{x})).$$

In words, the entropy parameters of any fixed points of density evolution, and so in particular the function h^{EBP}, are contained in the union of rectangles as given above.

Proof: The first two inequality follow from Lemma 10 and 11. From Lemma 10 we get $\mathtt{x} = H(\mathsf{f}) = H(T_{\mathtt{h}}(\mathsf{f})) \geq \mathtt{h}\,\underline{l}(\underline{r}(\mathtt{x}))$ which gives the upper bound on $\mathtt{h}$. Analogously,

Lemma 11 implies $\mathtt{x} \geq \overline{l}(\mathtt{h}, \overline{r}(\mathtt{x}))$. Since $\overline{l}(\mathtt{h}, \overline{r}(\mathtt{x}))$ is monotonically increasing in $\mathtt{h}$, this relation can be inverted as in the thesis of the theorem.

Given the fixed point $\mathtt{f}$, the corresponding EXIT entropy at variable nodes is $h^{\text{EBP}} = H(L(\rho(\mathtt{f})))$. The bounds are obtained as in the proofs of Lemmas 10 and 11. ∎

Discussion: The bounds given above are by no means best possible. First, the given bounds are "universal" in the sense that the are valid for *all* channel distributions. Better bounds for any specific channel family can be derived by taking the actual input distribution into account. Even in the universal case slightly better bounds can be given by taking into account that at the variable node before convolution with the channel, the incoming message density can not be of arbitrary shape but that it is already the convolution of several message densities. Second, tighter bounds on the extremes of information combining have been derived in [34] and can be translated to giver tighter bounds on EXIT functions, albeit at the prize of more complex expressions. Finally, by using a similar techniques one can also give bounds on the entropy versus GEXIT parameter of any fixed point with respect to any smooth channel family.

Example 22 (LDPC$(2/5x + 3/5x^5, x^5)$): Consider again the dd pair $(\lambda, \rho) = (2/5x + 3/5x^5, x^5)$. Fig. 13 shows on the left the construction of the bounded region (union of rectangles) which contains all EBP GEXIT curves. The dashed lines represent the individual curves traced out by the corner points of the rectangles. On the right this is compared to the actual EBP GEXIT curves for transmission over the BSC and the BEC families (solid lines).

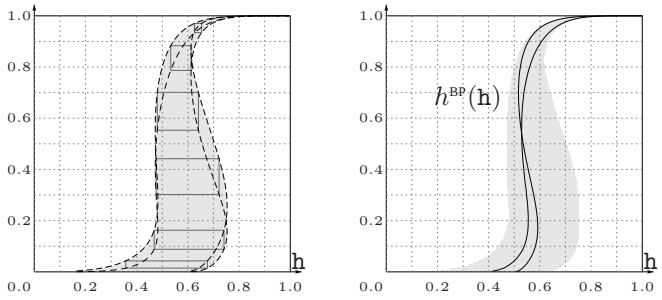

Fig. 13. Left: Construction of bounding region for all EBP EXIT curves for the dd pair $(\lambda, \rho) = (2/5x + 3/5x^5, x^5)$. Right: The EBP EXIT curves for transmission over the BSC and the BEC families.

Theorem 8 (EPP Area Theorem): Consider the dd pair (λ, ρ) and transmission over the smooth and degraded family $\{\text{BMS}(\mathtt{h})\}$. Let g^{EBP} denote the corresponding EBP GEXIT function. Assume that the corresponding $\{\mathtt{f_x}\}_\mathtt{x}$ and $\{\mathtt{c_x}\}_\mathtt{x}$, $\mathtt{x} \in [0, 1]$, form a *complete fixed-point family*. Then

$$\int_0^1 g^{\text{EBP}}(\mathtt{x})\mathrm{d}\mathtt{x} = 1 - \frac{\int \rho}{\int \lambda}.$$

Proof: First, let us assume that the ensemble is $(\mathtt{l}, \mathtt{r})$-regular. Consider a variable node and the corresponding computation tree of depth one as shown in Fig. 14. Let us assume that the bit associated to the root node is passed through the channel characterized by $\mathtt{c_x}$, while the ones associated to the leaf nodes are passed through a channel characterized by $\mathtt{f_x}$. Apply the GAT: let $X = (X_1, \ldots, X_{1+\mathtt{l}\times(\mathtt{r}-1)})$ be the transmitted codeword chosen uniformly at random from the tree code and $Y(\mathtt{x})$ be the result of passing the bits of X through their respective channels with parameter $\mathtt{x}$. Note that $H(X \,|\, Y(\mathtt{x} = 1)) - H(X \,|\, Y(\mathtt{x} = 0)) = H(X)$. This follows since by assumption the fixed-point family is complete. In particular this implies that the channel for $\mathtt{x} = 0$ is the "noiseless" channel so that $H(X \,|\, Y(\mathtt{x} = 0)) = 0$. By the GAT, this difference is equal to the sum of the integrals of the individual g_i curves, where the integral extends from $\mathtt{x} = 0$ to $\mathtt{x} = 1$. There are two types of individual g_i curves, namely the one associated to the root node, call it g_r, and the $\mathtt{l}(\mathtt{r}-1)$ ones associated to the leaf nodes, call them g_l. To summarize, the GAT states

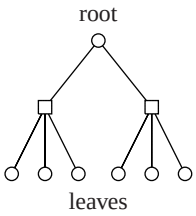

Fig. 14. Computation tree of depth one for the $(2, 4)$-regular LDPC ensemble.

$$H(X) = \int_0^1 g_\mathrm{r}(\mathtt{x})\,\mathrm{d}\mathtt{x} + \mathtt{l}(\mathtt{r}-1)\int_0^1 g_\mathrm{l}(\mathtt{x})\mathrm{d}\mathtt{x}.$$

Note that $H(X) = 1 + \mathtt{l}(\mathtt{r}-1) - \mathtt{l} = 1 - \mathtt{l}(\mathtt{r}-2)$ since the computati on tree contains $1 + \mathtt{l}(\mathtt{r}-1)$ variable nodes and $\mathtt{l}$ check nodes. Moreover, $\int_0^1 g_\mathrm{l}(\mathtt{x})\mathrm{d}\mathtt{x} = \int_0^1 1 - \rho(1 - \mathtt{x})\mathrm{d}\mathtt{x} = (\mathtt{r}-1)/\mathtt{r}$. This follows by applying the GAT once again to a $[\mathtt{r}, 1, \mathtt{r}-1]$ single parity check code. Collecting these observations and solving for $\int_0^1 g_\mathrm{r}(\mathtt{x})\,\mathrm{d}\mathtt{x}$, we get

$$\int_0^1 g_\mathrm{r}(\mathtt{x})\,\mathrm{d}\mathtt{x} = 1 - \mathtt{l}/\mathtt{r} = r,$$

as claimed since $g_\mathrm{r} = g^{\text{EBP}}$.

The irregular case follows in the same manner: we consider the ensemble of computation trees of depth one where the degree of the root note is chosen according to the node degree distribution Λ and each edge emanating from this root node is connected to a check node whose degree is chosen according to the edge degree distribution ρ. As before, leaf nodes experience the channel characterized by $\mathtt{f}_x$, whereas the root node experiences the channel characterized by $\mathtt{c}_x$. We apply the GAT to each such choice and average with the respective probabilities. ∎

This result imposes some strong constraint on BP GEXIT functions and their relation to MAP GEXIT functions. Here is an example.

Corollary 3: Consider communication over the smooth and degraded family $\{\text{BMS}(\mathtt{h})\}_\mathtt{h}$, $\mathtt{h} \in [0, 1]$ using uniformly random codes from the ensemble LDPC(n, λ, ρ) and assume that the rate of this ensemble converges to the design rate, see [5, Lemma 7]. Assume that the BP fixed point family $\{\text{BMS}(\mathtt{h}), \mathtt{a_h}\}$, is smooth and complete. Then (MAP) GEXIT

function and BP GEXIT function coincide: $g(\mathtt{h}) = g^{\text{BP}}(\mathtt{h})$ for almost every $\mathtt{h} \in [0,1]$.

Proof: By hypothesis we can apply Theorem 8 to the BP GEXIT function. We get

$$\int_0^1 g^{\text{BP}}(\mathtt{h})\,\mathrm{d}\mathtt{h} = r\,.$$

Further, by the GAT (and applying Fubini theorem and Fatou's lemma as in the proof of Theorem 5)

$$\int_0^1 g(\mathtt{h})\,\mathrm{d}\mathtt{h} = r\,.$$

The proof if completed by noticing that, because of Lemma 9, $g(\mathtt{h}) \le g^{\text{BP}}(\mathtt{h})$ for every $\mathtt{h} \in [0,1]$. ∎

Proving that the hypotheses of this Corollary hold for some dd pair (λ, ρ) is a challenging task (see also next section). On the other hand, numerical computations show very clearly that this is the case, for instance, for cycle ensembles, cf. Example 17.

IX. Regularity of Extended BP GEXIT Curves

Theorem 6 ensures (for many LDPC ensembles) the existence of a fixed point pair $(\mathsf{f}_{\mathtt{x}}, \mathsf{c}_{\mathtt{x}})$ for each value of $\mathtt{x} = H(\mathsf{f}_{\mathtt{x}})$. However, for applying the extended Area Theorem 8 the resulting family has to be smooth with respect to the parameter $\mathtt{x}$. That this is indeed the case is strongly suggested by the numerical computation of the EBP curve, cf. Sec. VII. We provide here some partial analytic results in this direction.

Throughout this section, we denote by $\mathfrak{B}(\mathsf{a})$ the Battacharyya parameter for the L-density a. Furthermore, when assuming communication through the channel BMS$(\mathtt{h})$, we denote by $B_{\mathtt{h}}$ the Battacharyya parameter of the channel.

Lemma 12: Assume communication over the degraded family $\{\text{BMS}(\mathtt{h})\}_{\mathtt{h}}$ channel using the dd pair (λ, ρ). Then, for any $\mathtt{h}$, there exists at most a unique fixed point density $\mathsf{f}_{\mathtt{h}}$ such that

$$B_{\mathtt{h}} \lambda'(1) \rho''(1 - \mathfrak{B}(\mathsf{f}_{\mathtt{h}})^2) < 1\,. \tag{18}$$

Furthermore, if such a density $\mathsf{f}_{\mathtt{h}}$ exists, it coincides with the BP fixed point. Finally, $\mathfrak{B}(\mathsf{f}_{\mathtt{h}})$ is Lipschitz continuous with respect to $B_{\mathtt{h}}$. More precisely, if the two fixed points $\mathsf{f}_{\mathtt{h}_1}$, $\mathsf{f}_{\mathtt{h}_2}$ satisfy the condition $B_{\mathtt{h}_i} \lambda'(1) \rho''(1 - \mathfrak{B}(\mathsf{f}_{\mathtt{h}_i})^2) \le 1 - \delta$ for some $\delta > 0$, then there exists $C = C(\delta, \lambda, \rho)$, such that

$$|\,\mathfrak{B}(\mathsf{f}_{\mathtt{h}_1}) - \mathfrak{B}(\mathsf{f}_{\mathtt{h}_2})| \le C\,|B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|\,.$$

Proof: Consider two channel parameters $\mathtt{h}_1 \le \mathtt{h}_2$ and two L-densities a_1 and a_2 satisfying the condition $B_{\mathtt{h}_i} \lambda'(1) \rho''(1 - \mathfrak{B}(\mathsf{f}_{\mathtt{h}_i})^2) < 1 - \delta$ for some $\delta > 0$. Assume that a_2 is physically degraded with respect to a_1. We prove in Appendix III that there exists a constant $\alpha = \alpha(\lambda, \rho, \delta) < 1$ on δ, the channel family and the degree distribution, such that

$$\begin{aligned} |\,\mathfrak{B}(T_{\mathtt{h}_1}(\mathsf{a}_1)) - \mathfrak{B}(T_{\mathtt{h}_2}(\mathsf{a}_2))| \le \\ \alpha\,|\,\mathfrak{B}(\mathsf{a}_1) - \mathfrak{B}(\mathsf{a}_2)| + |B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|\,. \end{aligned} \tag{19}$$

Let us show that this result implies the thesis. Denote by $\mathsf{f}_{\mathtt{h}}$ the BP fixed point for the channel BMS$(\mathtt{h})$ and notice that any other fixed point $\mathsf{f}'_{\mathtt{h}}$ for the same channel is necessarily physically upgraded with respect to $\mathsf{f}_{\mathtt{h}}$. Using the standard notation $\mathsf{f}_{\mathtt{h}} \succ \mathsf{f}'_{\mathtt{h}}$. In fact $\Delta_0 \succ \mathsf{f}'_{\mathtt{h}}$. By applying the density evolution operator, we deduce that $\mathsf{a}_{\mathtt{h}}^{\text{BP},\ell} \succ \mathsf{f}'_{\mathtt{h}}$, where $\mathsf{a}^{\text{BP},\ell}$ is the density after ℓ iterations of BP. By taking the limit $\ell \to \infty$ we get $\mathsf{f}_{\mathtt{h}} \succ \mathsf{f}'_{\mathtt{h}}$.

Next notice that, if $\mathsf{f}_{\mathtt{h}}$ satisfies Eq. (18) there cannot be a distinct fixed point, physically upgraded with respect to $\mathsf{f}_{\mathtt{h}}$, also satisfying Eq. (18). If such a density $\mathsf{f}'_{\mathtt{h}}$ existed, we could apply (19) to get

$$|\,\mathfrak{B}(T_{\mathtt{h}}(\mathsf{f}_{\mathtt{h}})) - \mathfrak{B}(T_{\mathtt{h}}(\mathsf{f}'_{\mathtt{h}}))| \le \alpha\,|\,\mathfrak{B}(\mathsf{f}_{\mathtt{h}}) - \mathfrak{B}(\mathsf{f}'_{\mathtt{h}})|\,,$$

with $\alpha < 1$. But, since $T_{\mathtt{h}}(\mathsf{f}_{\mathtt{h}}) = \mathsf{f}_{\mathtt{h}}$ and $T_{\mathtt{h}}(\mathsf{f}'_{\mathtt{h}}) = \mathsf{f}'_{\mathtt{h}}$, this would imply $\mathfrak{B}(\mathsf{f}_{\mathtt{h}}) = \mathfrak{B}(\mathsf{f}'_{\mathtt{h}})$ which is impossible because $\mathsf{f}_{\mathtt{h}} \succ \mathsf{f}'_{\mathtt{h}}$.

Let us finally prove Lipschitz continuity, cf. Eq. (19). Under our hypotheses, the two fixed points $\mathsf{f}_{\mathtt{h}}$, $\mathsf{f}_{\mathtt{h}'}$ are the BP fixed points for channels BMS$(\mathtt{h})$ and BMS$(\mathtt{h}')$. Consider therefore the BP sequences $\{\mathsf{a}_{\mathtt{h}}^{\text{BP},\ell}\}_{\ell \ge 0}$, $\{\mathsf{a}_{\mathtt{h}'}^{\text{BP},\ell}\}_{\ell \ge 0}$. For each ℓ, $\mathsf{a}_{\mathtt{h}}^{\text{BP},\ell}$ (respectively $\mathsf{a}_{\mathtt{h}'}^{\text{BP},\ell}$) is physically degraded with respect to $\mathsf{f}_{\mathtt{h}}$ (respectively $\mathsf{f}_{\mathtt{h}'}$), and therefore satisfies the condition (18), since the latter does. Furthermore, assuming without loss of generality $\mathtt{h}' > \mathtt{h}$, we have $\mathsf{a}_{\mathtt{h}'}^{\text{BP},\ell} \succ \mathsf{a}_{\mathtt{h}}^{\text{BP},\ell}$. Let $\delta_\ell \triangleq |\,\mathfrak{B}(\mathsf{a}_{\mathtt{h}}^{(\ell)} - \mathfrak{B}(\mathsf{a}_{\mathtt{h}'}^{(\ell)})|$. Clearly $\delta_0 = 0$. By applying Eq. (19), we get $\delta_{\ell+1} \le \alpha\,\delta_\ell + |B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|$, and therefore

$$\delta_\ell \le (\alpha + \alpha^2 + \cdots + \alpha^\ell)\,|B_{\mathtt{h}_1} - B_{\mathtt{h}_2}| \le \frac{\alpha}{1-\alpha}\,|B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|\,.$$

The thesis follows by taking the $\ell \to \infty$ limit. ∎

It is worth mentioning that the Lipschitz condition Eq. (19) implies analogous regularity properties for other functionals of the density $\mathsf{a}_{\mathtt{h}}$. For instance, it is easy to show that $|H(\mathsf{f}_{\mathtt{h}_1}) - H(\mathsf{f}_{\mathtt{h}_2})| \le A\,|\,\mathfrak{B}(\mathsf{f}_{\mathtt{h}_1}) - \mathfrak{B}(\mathsf{f}_{\mathtt{h}_2})|$, for some universal constant A. Also, the Battacharyya parameter is, for most channel families, a smooth function of the channel parameter. Regularity with respect to $B_{\mathtt{h}}$ translates therefore immediately into regularity with respect to $\mathtt{h}$.

In applying the above result, it is helpful to have bounds on the Battacharyya parameter of the fixed point densities.

Lemma 13: Assume communication over the channel BMS$(\mathtt{h})$ using random codes from the (λ, ρ) ensemble. If f is a fixed point density with Battacharyya parameter $b = \mathfrak{B}(\mathsf{f})$, then

$$b \ge B_{\mathtt{h}} \lambda(\tilde{b})\,, \qquad \tilde{b} \triangleq \sum_{\mathtt{r}} \rho_{\mathtt{r}} \sqrt{1 - (1-b^2)^{\mathtt{r}-1}}\,.$$

Proof: First notice that $b = B_{\mathtt{h}} \lambda(\tilde{b}')$ where $\tilde{b} \triangleq \sum_{\mathtt{r}} \rho_{\mathtt{r}}\,\mathfrak{B}(\mathsf{f}^{\boxtimes(\mathtt{r}-1)})$, and $\boxtimes$ denotes the convolution at check nodes. It is convenient to write densities in terms of the variable $u \triangleq \sqrt{1 - \tanh^2(x/2)}$. With a slight abuse of notation, we use the same symbol f to denote the density with respect to u. We get

$$\mathfrak{B}(\mathsf{f}^{\boxtimes i}) = \int \sqrt{1 - (1-u_1^2)\cdots(1-u_i)^2}\,\mathsf{f}(u_1)\mathrm{d}u_1 \cdots \mathsf{f}(u_i)\mathrm{d}u_i\,.$$

The proof is completed by using convexity with respect to the $u_1, \ldots u_i$ together with the fact that $b = \int u \mathsf{f}(u)\,\mathrm{d}u$. ∎

Example 23: Consider the $(2,3)$ ensemble and communication over the BSC(ϵ). In this case Eq. (18) is equivalent to

$$\mathfrak{B}(\mathsf{f}) > \sqrt{1 - \frac{1}{2B(\epsilon)}}\,, \tag{20}$$

where $B(\epsilon)$ denotes the channel Battacharyya parameter as a function of the flip probability $B(\epsilon) = \sqrt{4\epsilon(1-\epsilon)}$. Lemma 13 implies (if we neglect the case $\mathfrak{B}(\mathsf{f}) = 0$ which corresponds to a no-error fixed point) $\mathfrak{B}(\mathsf{f}) \geq \sqrt{2 - B(\epsilon)^{-2}}$. This lower bound lies in the region described by equation (20) as soon as $B(\epsilon) \geq (\sqrt{17}-1)/4$, i.e., $\epsilon > \epsilon_*$ with

$$\epsilon_* = \frac{1}{2} - \sqrt{\frac{\sqrt{17}-1}{32}}\,,$$

which yields $\epsilon_* \approx 0.18759473$. The above results imply that a unique fixed point density (apart from the no-error one) exists for any $\epsilon > \epsilon_*$. On the other hand numerical computations suggest this to be the case for all values above the local stability threshold $\epsilon_{\rm ls} = (2-\sqrt{2})/4 \approx 0.066987298$. Fig. 15 shows the Battacharyya constant of the fixed point density as a function of the channel parameter of the BSC (solid line), the bound stated in (20) (dotted line), as well as the bound $\mathfrak{B}(\mathsf{f}) \geq \sqrt{2 - B(\epsilon)^{-2}}$ (dashed line).

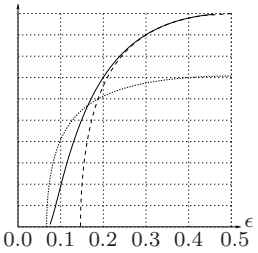

Fig. 15. The solid line shows the Battacharyya constant of the fixed point density as a function of the channel parameter of the BSC. The dotted line corresponds to the bound stated in (20), whereas the dashed curve corresponds to the bound $\mathfrak{B}(\mathsf{f}) \geq \sqrt{2 - B(\epsilon)^{-2}}$.

As stressed in the previous section, EBP curves are expected to be single valued smooth functions of the entropy $H(\mathsf{f})$ of the fixed point density. The same expectation holds, if entropy is replaced by any linear functional which preserves physical degradation. The following result confirms that better regularity properties can indeed be obtained by taking this point of view.

Lemma 14: Let $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$ be a degraded family. Assume f_1 and f_2 to be fixed point densities for the channel parameters $\mathtt{h}_1$, $\mathtt{h}_2$, and that f_1 is physically degraded with respect to f_2. If $\mathfrak{B}(\mathsf{f}_1) \geq \delta > 0$, then there exists a constant $C = C(\lambda, \rho, \delta)$ such that

$$|B_{\mathtt{h}_1} - B_{\mathtt{h}_2}| \leq C\,|\,\mathfrak{B}(\mathsf{f}_1) - \mathfrak{B}(\mathsf{f}_2)|\,.$$

In words, the channel is a Lipschitz continuous function of the Battacharyya parameter of the fixed point density.

Proof: Proceeding as in the proof of Eq. (19), cf. Appendix III it is easy to show that, if $\mathsf{a}_1 \succ \mathsf{a}_2$, then

$$|\,\mathfrak{B}(T_1(\mathsf{a}_1)) - \mathfrak{B}(T_1(\mathsf{a}_2))| \leq \lambda'(1)\rho''(1)|\,\mathfrak{B}(\mathsf{a}_1) - \mathfrak{B}(\mathsf{a}_2)|\,.$$

Furthermore, if $\mathfrak{B}(\mathsf{a}) \geq \delta > 0$, then $\mathfrak{B}(T_1(\mathsf{a})) \geq \delta'$ for some $\delta' > 0$.

Consider now the difference $|\,\mathfrak{B}(T_{\mathtt{h}_1}(\mathsf{f}_1)) - \mathfrak{B}(T_{\mathtt{h}_2}(\mathsf{f}_2))|$. Since $\mathsf{f}_{1/2}$ are density evolution fixed points, this is equal to $|\,\mathfrak{B}(\mathsf{f}_1) - \mathfrak{B}(\mathsf{f}_2)|$. We get therefore

$$\begin{aligned}
|\,\mathfrak{B}(\mathsf{f}_1) - \mathfrak{B}(\mathsf{f}_2)| &= |B_{\mathtt{h}_1}\,\mathfrak{B}(T_1(\mathsf{f}_1)) - B_{\mathtt{h}_2}\,\mathfrak{B}(T_1(\mathsf{f}_2))| \\
&\geq |B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|\,\mathfrak{B}(T_1(\mathsf{f}_2)) - B_{\mathtt{h}_1}|\,\mathfrak{B}(T_1(\mathsf{f}_1)) - \mathfrak{B}(T_1(\mathsf{f}_2))| \\
&\geq |B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|\delta' - \lambda'(1)\rho''(1)|\,\mathfrak{B}(\mathsf{f}_1) - \mathfrak{B}(\mathsf{f}_2)|\,,
\end{aligned}$$

which implies the thesis after solving for $|B_{\mathtt{h}_1} - B_{\mathtt{h}_2}|$. ∎

X. MAP Versus BP Marginals

As we saw in Sections VII and VIII, the MAP and BP GEXIT curves are strictly related for LDPC codes in the large blocklength limit. We conjectured that they can be connected through the Maxwell construction. In particular, this would imply that they are asymptotically equal above the MAP threshold for a large family of ensembles, cf. for instance Example 18.

Does the coincidence of GEXIT curves mean that BP and MAP decoding in fact coincide *bit by bit*? More precisely, belief propagation can be regarded as a low complexity (approximate) algorithm for computing the marginal distributions $p_{X_i\,|\,Y}(x_i\,|\,y)$. It is well established [14], that the BP estimate is asymptotically correct in the low noise regime $\mathtt{h} < \mathtt{h}_{\rm BP}$. We wonder whether the same is true whenever the two GEXIT functions coincide.

Perhaps surprising, the answer is positive. In order to proceed, it is convenient to introduce some notations. For the sake of simplicity we consider the case of a binary channel. Rather than the marginal distributions $p_{X_i|Y}(x_i\,|\,y)$, it is convenient to focus on the extrinsic soft bits

$$\mu_i(y) \equiv \mathbb{E}[X_i\,|\,Y_{\sim i} = y_{\sim i}]\,.$$

We will further denote by $\mu_i^{{\rm BP},\ell}(y)$, the estimate of this quantity provided by BP, after ℓ iterations. Notice that $\mu_i(y) = \tanh\phi_i(y_{\sim i})$, and $\mu_i^{{\rm BP},\ell}(y) = \tanh\phi_i^{{\rm BP},\ell}(y_{\sim i})$.

A meaningful measure of how much 'incorrect' is BP, is the mean square error

$$\Delta^{(\ell)}(y) \equiv \frac{1}{n}\sum_{i=1}^{n}\left|\mu_i^{{\rm BP},\ell}(y) - \mu_i(y)\right|^2\,.$$

Let us stress that $\Delta^{(\ell)}(y)$ implies a rather strict notion of correctness. We are not just requiring the hard decision reached by BP to be (approximatively) the same that would be provided by a MAP decoder. Rather, BP should be able to reconstruct the full information about X_i, given the received message.

Our main result is presented below (here we refer to the Tanner graph associated to the code parity check matrix, which is naturally related to belief propagation).

Theorem 9: Consider communication using a linear code over a smooth channel $\mathrm{BMS}(\mathtt{h})$, and let Y be the channel output if the input is uniformly random codeword X. Let $|d|(\cdot)$ denote the GEXIT kernel in the $|D|$-domain and $K \equiv -\sup\left\{\frac{\mathrm{d}^2|d|(x)}{\mathrm{d}x^2} : x \in [0,1]\right\} > 0$. Assume that, for a uniformly random variable node i in the Tanner graph, the shortest loop through i has length larger than 2ℓ with probability at least $1-\delta$. Then

$$\mathbb{E}\,\Delta^{(\ell)}(Y) \leq \frac{2}{K}[g^{{\rm BP},\ell}(\mathtt{h}) - g(\mathtt{h})] + 4\delta\,.$$

Let us stress that this result holds, not just for random elements of an $\mathrm{LDPC}(n,\lambda,\rho)$ ensemble, but for any code with the prescribed sparseness properties.

The proof makes use of a technical lemma, which we state below, and prove in Appendix IV.

Lemma 15: Consider a random variable X taking values in $\{+1,-1\}$ and assume that $X \to Y \to Z$ forms a Markov chain. Let $k:[0,1]\to\mathbb{R}$ be twice differentiable with $k'(0)\le 0$, and $k''(x)\le -K<0$ for any $x\in[0,1]$. If we denote $\mu_{\mathsf{Y}}(y)=\mathbb{E}[X\,|\,Y=y]$ and $\mu_{\mathsf{Z}}(z)=\mathbb{E}[X\,|\,Z=z]$, then

$$\mathbb{E}[k(|\mu_{\mathsf{Y}}(Y)|)] \le \mathbb{E}[k(|\mu_{\mathsf{Z}}(Z)|)] - \frac{1}{2}\,K\,\mathbb{E}[|\mu_{\mathsf{Y}}(Y)-\mu_{\mathsf{Z}}(Z)|^2]\,.$$

Proof: [Theorem 9] The MAP GEXIT function can be written as

$$g(\mathtt{h}) = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[|d|\,(|\mu_i(Y)|)]\,.$$

An analogous expression holds for the BP GEXIT function if we replace $\mu_i(Y)$ with $\mu_i^{\scriptscriptstyle \mathrm{BP},\ell}(Y)$. We claim that, if the shortest loop through i in the Tanner graph is longer than 2ℓ, then

$$\begin{aligned}\mathbb{E}[|d|\,(|\mu_i(Y)|)] \le& \mathbb{E}[|d|\,(|\mu_i^{\scriptscriptstyle \mathrm{BP},\ell}(Y)|)] - \\ &- \frac{1}{2}\,K\,\mathbb{E}[(\mu_i(Y)-\mu_i^{\scriptscriptstyle \mathrm{BP},\ell}(Y))^2]\,.\end{aligned} \tag{21}$$

The thesis follows by rearranging the terms, using the trivial bound $(\mu_i(Y)-\mu_i^{\scriptscriptstyle \mathrm{BP},\ell}(Y))^2\le 4$ whenever the shortest loop through i is not longer than 2ℓ and summing over i.

In order to prove the above claim, let $Y_{\sim i}^{(\ell)}$ denote the subset of received signals within a distance ℓ from the variable node i on the Tanner graph. Notice that $X_i \to Y_{\sim i} \to Y_{\sim i}^{(\ell)}$ is a Markov chain, and that $\mu_i(Y)=\mathbb{E}[X_i|Y_{\sim i}]$, $\mu_i^{(\ell)}(Y)=\mathbb{E}[X_i|Y_{\sim i}^{(\ell)}]$. We can therefore apply Lemma 15, with $k(x)=|d|(x)$. This yields Eq. (21), and thus concludes the proof. ■

One may wonder whether the distortion measure $\Delta^{(\ell)}(y)$ is appropriate. One could, for instance consider the actual soft bits, rather than the extrinsic ones. If we let $\tilde{\mu}_i(y)=\mathbb{E}[X_i|Y=y]$, and denote as $\tilde{\mu}_i^{\scriptscriptstyle \mathrm{BP},\ell}(y)$ the corresponding BP estimate, we may define

$$\widetilde{\Delta}^{(\ell)}(y) = \frac{1}{n}\sum_{i=1}^{n}\left|\tilde{\mu}_i^{\scriptscriptstyle \mathrm{BP},\ell}(y)-\tilde{\mu}_i(y)\right|^2\,.$$

Recall that hard decoding decisions are taken in terms of $\tilde{\mu}_i(y)$, rather than $\mu_i(y)$. We are therefore interested in knowing whether $\widetilde{\Delta}^{(\ell)}(y)$ can be much larger than $\Delta^{(\ell)}(y)$. The answer is generically negative, as shown by the lemma below.

Lemma 16: Assume communication over a BMS channel with L-density $\mathsf{c}(l)$. Then

$$\mathbb{E}\,\widetilde{\Delta}^{(\ell)}(Y) \le C\,\mathbb{E}\,\Delta^{(\ell)}(Y)$$

where $C\equiv\int e^{2|l|}\mathsf{c}(l)\,\mathrm{d}l$.

The proof is deferred to Appendix IV.

Theorem 9 obviously imply that belief propagation is 'asymptotically correct' every time the BP and MAP GEXIT functions asymptotically coincide. We conjectured in Section VII that the MAP GEXIT function can be obtained from the EBP one through the Maxwell construction. This construction allows therefore to determine in which domain of $\mathtt{h}$ BP and MAP GEXIT functions do coincide. It is worth stating the final result explicitly for a few simple cases cases.

Corollary 4: Consider communication over degraded, smooth and complete family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$, using uniformly random codes from the ensemble $\mathrm{LDPC}(n,\lambda,\rho)$ and assume that the rate of this ensemble converges to the design rate. Assume that the BP fixed point family $\{\mathrm{BMS}(\mathtt{h}),\mathtt{a}_{\mathtt{h}}\}$, is smooth and complete. Then, for almost every $\mathtt{h}\in[0,1]$

$$\lim_{\ell\to\infty}\lim_{n\to\infty}\mathbb{E}\,\Delta^{(\ell)}(Y)=0\,.$$

The proof follows easily from Corollary 3.

A somewhat more general statement is the following.

Corollary 5: Consider communication over over degraded, smooth and complete family $\{\mathrm{BMS}(\mathtt{h})\}_{\mathtt{h}}$, using uniformly random codes from the ensemble $\mathrm{LDPC}(n,\lambda,\rho)$ and assume that the rate of this ensemble converges to the design rate. Assume that the upper bound in on the MAP threshold in Theorem 5 is tight: $\mathtt{h}^{\scriptscriptstyle \mathrm{MAP}}=\overline{\mathtt{h}}$. Then, for almost any $\mathtt{h}\in[\overline{\mathtt{h}},1]$,

$$\lim_{\ell\to\infty}\lim_{n\to\infty}\mathbb{E}\,\Delta^{(\ell)}(Y)=0\,.$$

Proof: Proceeding as in the proof of Theorem 5, one obtain that

$$\int_{\overline{\mathtt{h}}}^{1} g(\mathtt{h})\,\mathrm{d}\mathtt{h} = \int_{\overline{\mathtt{h}}}^{1} g^{\scriptscriptstyle \mathrm{BP}}(\mathtt{h})\,\mathrm{d}\mathtt{h} = r\,.$$

Since $g(\mathtt{h})\le g^{\scriptscriptstyle \mathrm{BP}}(\mathtt{h})$ for all $\mathtt{h}$, we have necessarily $g(\mathtt{h})=g^{\scriptscriptstyle \mathrm{BP}}(\mathtt{h})$ for almost any $\mathtt{h}\in[\overline{\mathtt{h}},1]$. The thesis follows by applying Theorem 9. ■

XI. Why We Can Not Surpass Capacity: The Matching Condition

The upper bound $\overline{\mathtt{h}}$ on the MAP threshold, cf. Theorem 5 cannot be larger than the Shannon threshold $1-r$. This follows by noticing that the GEXIT kernel is not larger than 1, and implies that iterative coding systems do not allow to communicate reliably above capacity. Of course, this result is also a straightforward consequence of Shannon's channel coding theorem. In this section we shall provide yet another proof of this basic fact. The interest of the new proof is threefold: (i) it does not assume communication over a smooth channel family; (ii) it uses only quantities appearing in density evolution (and not just fixed points); (iii) component codes (and their 'matching') play a crucial role.

For general BMS channels, and motivated by the geometric statement observed for the BEC and the relationship between the derivative of the mutual information and the MSE introduced by [7], [26], a similar chart, called MSE chart was constructed by Bhattad and Narayanan [35]. Assuming that the input densities to the component codes are Gaussian, this chart again fulfills the Area Theorem. In order to apply the MSE chart in the context of iterative coding the authors proposed to approximate the intermediate densities which appear in density evolution by "equivalent" Gaussian densities. This was an important first step in generalizing the matching condition to the whole class of BMS channels. In the following we show how to overcome the need for making the Gaussian approximation by using GEXIT functions.

To start, let us review the case of transmission over the BEC($\mathtt{h}$) using a degree distribution pair (λ, ρ). In this case density evolution is equivalent to the EXIT chart approach and the condition for successful decoding under BP reads

$$c(x) \triangleq 1 - \rho(1-x) \leq \lambda^{-1}(x/\mathtt{h}) \triangleq v_{\mathtt{h}}^{-1}(x).$$

This is shown in Fig. 16 for the degree distribution pair $(\lambda(x) = x^3, \rho(x) = x^4)$. The area under the curve $c(x)$ equals

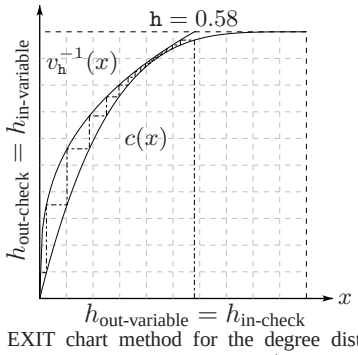

Fig. 16. The EXIT chart method for the degree distribution $(\lambda(x) = x^3, \rho(x) = x^4)$ and transmission over the BEC($\mathtt{h} = 0.58$).

$1 - \int \rho$ and the area to the left of the curve $v_{\mathtt{h}}^{-1}(x)$ is equal to $\mathtt{h} \int \lambda$. By the previous remarks, a necessary condition for successful BP decoding is that these two areas do not overlap. Since the total area equals 1 we get the necessary condition $\mathtt{h} \int \lambda + 1 - \int \rho \leq 1$. Rearranging terms, this is equivalent to the condition

$$1 - C_{\text{Sh}} = \mathtt{h} \leq \frac{\int \rho}{\int \lambda} = 1 - r(\lambda, \rho).$$

In words, the design rate $r(\lambda, \rho)$ of any LDPC ensemble which, for increasing block lengths, allows successful decoding over the BEC($\mathtt{h}$), can not surpass the Shannon limit $1 - \mathtt{h}$. An argument very similar to the above was introduced by Shokrollahi and Oswald [36], [37] (albeit not using the language and geometric interpretation of EXIT functions and applying a slightly different range of integration). It was the first bound on the performance of iterative systems in which the Shannon capacity appeared explicitly using only quantities of density evolution. A substantially more general version of this bound can be found in [16], [38], [39]. The extension to parallel turbo schemes is addressed in [40], [41]. See also [42].

Although the final result (namely that transmission above capacity is not possible) is trivial, the method of proof is well worth the effort since it shows how capacity enters in the calculation of the performance of iterative coding systems. By turning this bound around, we can find conditions under which iterative systems achieve capacity: In particular it shows that the two component-wise EXIT curves have to be matched perfectly. Indeed, all currently known capacity achieving degree-distributions for the BEC can be derived by starting with this perfect matching condition and working backwards. Let us now show that, by using component-wise GEXIT functions, the perfect matching condition holds in the general case. This might in the future serve as a starting point to find capacity-achieving degree distributions for general BMS channels. We need one preliminary definition.

Definition 9 (Interpolating Channel Families): Consider a degree distribution pair (λ, ρ) and transmission over the BMS channel characterized by its L-density c. Let $\mathsf{a}_{-1} = \Delta_0$ and $\mathsf{a}_0 = \mathsf{c}$ and set a_α, $\alpha \in [-1, 0]$, to $\mathsf{a}_\alpha = -\alpha \mathsf{a}_{-1} + (1+\alpha)\mathsf{a}_0$. The *interpolating density evolution families* $\{\mathsf{a}_\alpha\}_{\alpha=-1}^{\infty}$ and $\{\mathsf{b}_\alpha\}_{\alpha=0}^{\infty}$ are then defined as follows:

$$\mathsf{b}_\alpha = \sum_i \rho_i \mathsf{a}_{\alpha-1}^{\boxplus(i-1)}, \qquad \alpha \geq 0,$$
$$\mathsf{a}_\alpha = \sum_i \lambda_i \mathsf{c} \star \mathsf{b}_\alpha^{\star(i-1)}, \qquad \alpha \geq 0,$$

where $\star$ denotes the standard convolution of densities and $\mathsf{a} \boxplus \mathsf{b}$ denotes the density at the output of a check node, assuming that the input densities are a and b, respectively.

Discussion: First note that a_ℓ (b_ℓ), $\ell \in \mathbb{N}$, represents the sequence of L-densities of density evolution emitted by the variable (check) nodes in the ℓ-th iteration. By starting density evolution not only with $\mathsf{a}_0 = \mathsf{c}$ but with all possible convex combinations of Δ_0 and c, this discrete sequence of densities is completed to form a continuous family of densities ordered by physical degradation. The fact that the densities are ordered by physical degradation can be seen as follows: note that the computation tree for a_α can be constructed by taking the standard computation tree of $\mathsf{a}_{\lceil\alpha\rceil}$ and independently erasing the observation associated to each variable leaf node with probability $\lceil\alpha\rceil - \alpha$. It follows that we can convert the computation tree of a_α to that of $\mathsf{a}_{\alpha-1}$ by erasing all observations at the leaf nodes and by independently erasing each observation in the second (from the bottom) row of variable nodes with probability $\lceil\alpha\rceil - \alpha$. The same statement is true for b_α. If $\lim_{\ell\to\infty} H(\mathsf{a}_\ell) = 0$, i.e., if BP decoding is successful in the limit of large blocklengths, then the families are both complete.

Example 24 (Density Evolution and Interpolation): Consider transmission over the BSC($\epsilon = 0.07$) using a $(3, 6)$-regular ensemble. Fig. 17 depicts the density evolution process for this case. This process gives rise to

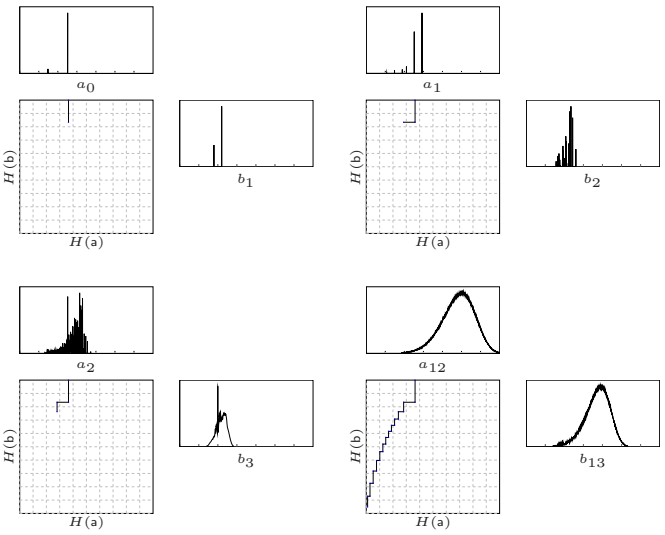

Fig. 17. Density evolution for $(3, 6)$-regular ensemble over BSC(0.07).

the sequences of densities $\{\mathsf{a}_\ell\}_{\ell=0}^{\infty}$, and $\{\mathsf{b}_\ell\}_{\ell=1}^{\infty}$. Fig. 18

shows the interpolation of these sequences for the choices $\alpha = 1.0, 0.95, 0.9$ and 0.8 and the complete such family.

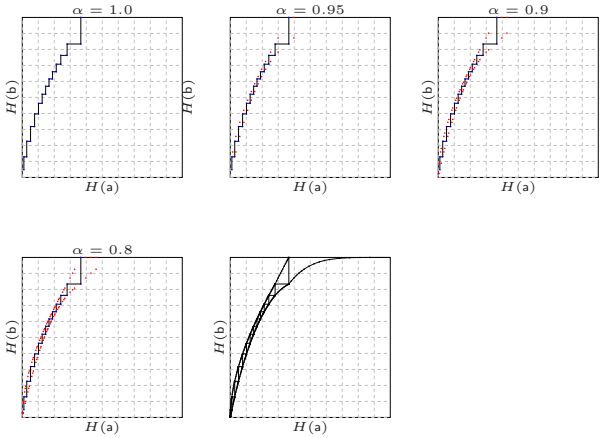

Fig. 18. Interpolation of densities.

Lemma 17: Consider a degree distribution pair (λ, ρ) and transmission over an BMS channel characterized by its L-density c so that density evolution converges to Δ_∞. Let $\{\mathsf{a}_\alpha\}_{\alpha=-1}^{\infty}$ and $\{\mathsf{b}_\alpha\}_{\alpha=0}^{\infty}$ denote the interpolated families as defined in Definition 9.

Then the two GEXIT curves parameterized by

$$\{H(\mathsf{a}_\alpha), G(\mathsf{a}_\alpha, \mathsf{b}_{\alpha+1})\}, \qquad \text{GEXIT of check nodes}$$
$$\{H(\mathsf{a}_\alpha), G(\mathsf{a}_\alpha, \mathsf{b}_\alpha)\}, \qquad \text{inverse of dual GEXIT of variable nodes}$$

do not cross and faithfully represent density evolution. Further, the area under the "check-node" GEXIT function is equal to $1 - \int \rho$ and the area to the left of the "inverse dual variable node" GEXIT function is equal to $H(\mathsf{c}) \int \lambda$. It follows that $r(\lambda, \rho) \leq 1 - H(\mathsf{c})$, i.e., the design rate can not exceed the Shannon limit.

Proof: First note that $\{H(\mathsf{a}_\alpha), G(\mathsf{a}_\alpha, \mathsf{b}_{\alpha+1})\}$ is the standard GEXIT curve representing the action of the check nodes: a_α corresponds to the density of the messages *entering* the check nodes and $\mathsf{b}_{\alpha+1}$ represents the density of the corresponding output messages. On the other hand, $\{H(\mathsf{a}_\alpha), G(\mathsf{a}_\alpha, \mathsf{b}_\alpha)\}$ is the inverse of the dual GEXIT curve corresponding to the action at the variable nodes: now the input density to the check nodes is b_α and a_α denotes the corresponding output density.

The fact that the two curves do not cross can be seen as follows. Fix an entropy value. This entropy value corresponds to a density a_α for a unique value of α. The fact that $G(\mathsf{a}_\alpha, \mathsf{b}_\alpha) \geq G(\mathsf{a}_\alpha, \mathsf{b}_{\alpha+1})$ now follows from the fact that $\mathsf{b}_{\alpha+1} \prec \mathsf{b}_\alpha$ and that for any symmetric a_α this relationship stays preserved by applying the GEXIT functional according to Corollary 1.

The statements regarding the areas of the two curves follow in a straightforward manner from the GAT and Lemma 8. The bound on the achievable rate follows in the same manner as for the BEC: the total area of the GEXIT box equals one and the two curves do not overlap and have areas $1 - \int \rho$ and $H(\mathsf{c})$. It follows that $1 - \int \rho + H(\mathsf{c}) \int \lambda \leq 1$, which is equivalent to the claim $r(\lambda, \rho) \leq 1 - H(\mathsf{c})$. ∎

We see that the matching condition still holds for general channels. There are a few important differences between the general case and the simple case of transmission over the BEC. For the BEC, the intermediate densities are always the BEC densities independent of the degree distribution. This of course enormously simplifies the task. Further, for the BEC, given the two EXIT curves, the progress of density evolution is simply given by a staircase function bounded by the two EXIT curves. For the general case, this staircase function still has vertical pieces but the "horizontal" pieces have in general a non-vanishing slope. This is true since the y-axis for the "check node" step measures $G(\mathsf{a}_\alpha, \mathsf{b}_{\alpha+1})$, but in the subsequent "inverse variable node" step it measures $G(\mathsf{a}_{\alpha+1}, \mathsf{b}_{\alpha+1})$. Therefore, one should think of two sets of labels on the y-axis, one measuring $G(\mathsf{a}_\alpha, \mathsf{b}_{\alpha+1})$, and the second one measuring $G(\mathsf{a}_{\alpha+1}, \mathsf{b}_{\alpha+1})$. The "horizontal" step then consists of first switching from the first y-axis to the second, so that the labels correspond to the same density b and then drawing a horizontal line until it crosses the "inverse variable node" GEXIT curve. The "vertical" step stays as before, i.e., it really corresponds to drawing a vertical line. All this is certainly best clarified by a simple example.

Example 25 ($(3, 6)$ Ensemble and Transmission over BSC): Consider the $(3, 6)$-regular ensemble and transmission over the BSC(0.07). The corresponding illustrations are shown in Fig. 19. The top-left figure shows the standard GEXIT curve for the check node side. The top-right figure shows the dual GEXIT curve corresponding to the variable node side. In order to use these two curves in the same figure, it is convenient to consider the inverse function for the variable node side. This is shown in the bottom-left figure. In the bottom-right figure both curves are shown together with the "staircase" like function which represents density evolution. As we see, the two curves to not overlap and have both the correct areas.

As remarked earlier, one potential use of the matching condition is to find capacity approaching degree distribution pairs. Let us quickly outline a further such potential application. Assuming that we have found a sequence of capacity-achieving degree distributions, how does the number of required iterations scale as we approach capacity. It has been conjectured that the the number of required iterations scales like $1/\delta$, where δ is the gap to capacity. This conjecture is based on the geometric picture which the matching condition implies. To make things simple, imagine the two GEXIT curves as two parallel lines, lets say both at a 45 degree angle, a certain distance apart, and think of density evolution as a staircase function. From the previous results, the area between the lines is proportional to δ. Therefore, if we half δ the distance between the lines has to be halved and one would expect that we need twice as many steps. Obviously, the above discussion was based on a number of simplifying assumptions. It remains to be seen if this conjecture can be proven rigorously.

XII. Conclusion

Since the introduction of EXIT functions for the analysis iterative coding systems [17]–[21], researchers have tried to

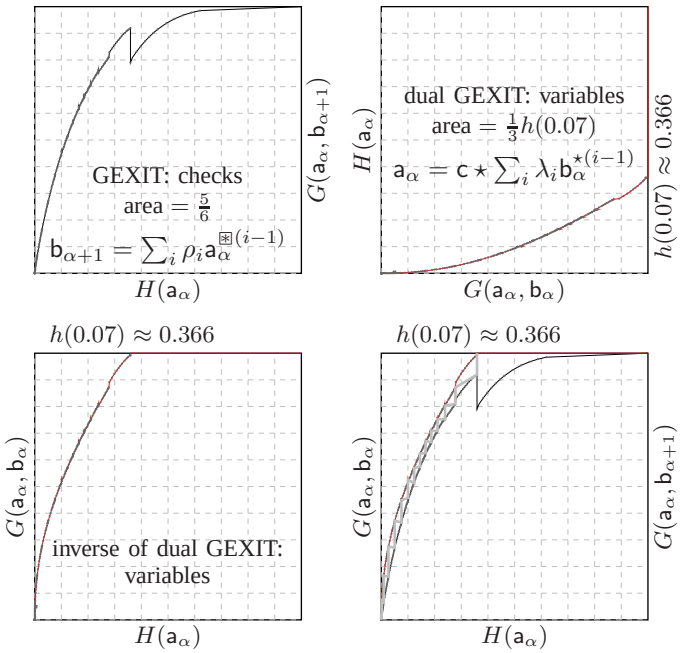

Fig. 19. Faithful representation of density evolution by two non-overlapping component-wise GEXIT functions which represent the "actions" of the check nodes and variable nodes, respectively. The area between the two curves is proportional to the additive gap to capacity.

substantiate theoretically the empirical area rules that these seemed to satisfy. In this paper we showed how to *prove* these rules in a very general setting. The price to pay was to replace EXIT functions by GEXIT functions. Fortunately, GEXIT functions are as simple to compute as ordinary EXIT functions and share in general many of their properties.

We also presented several applications of this new tool. Most notably: (i) It allows one to prove an upper bound on the MAP threshold which is conjectured to coincide with the actual threshold for several classes of ensembles (e.g. regular ones). (ii) Via extended BP GEXIT curves, it provides some constraints on the relation between BP and MAP decoding. These constraints lead naturally to the Maxwell construction which provides the precise connection between the two. In particular we found that the BP soft bit estimates are asymptotically exact for a noise range *above threshold*. (iii) It implies a matching constraint on component codes of capacity-achieving systems.

These results open many research directions. It may be worth to list a few of them.

Prove existence, uniqueness and regularity properties of asymptotic MAP and extended BP GEXIT curves. In particular, we expect that the last one is a smooth single valued function of the entropy of the fixed point density. The iterative procedure which we presented in Section VIII only *proves* that for each message entropy there is at least one fixed point of density evolution. But, empirically, when running this algorithm, we found that indeed there seems to be a unique such fixed point and that all these fixed points seem to form a smooth manifold. Further, we proved several partial results in this direction (for instance existence for EBP curves, uniqueness for MAP curves, etc). However, the general question remains open.

Prove that the Maxwell construction indeed provides the correct connection between MAP and BP GEXIT curves. As particular case (which may well be simpler than the general statement), prove the upper bound (5) is indeed tight for some selected ensembles, e.g. for regular ones.

Use the interpolation construction of Section XI to prove a lower bound on the number of message passing iterations as a function of the gap to capacity.

Acknowledgment

The authors would like to thank Nicolas Macris and Olivier Lévêque for useful discussions.

A.M. has been partially supported by the EU integrated project EVERGROW.

Appendix I
GEXIT Kernel over Gaussian Channels

This appendix contains a few useful results concerning the GEXIT kernel for Gaussian channels.

Lemma 18 (GEXIT Kernel, L-Domain – $\{BAWGNC(\mathtt{h})\}$): Consider the family $\{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}\}$ of BAWGN channels, where $\mathtt{h}$ denotes the channel entropy. The channel model is therefore $Y = X + N$, where X takes values $x \in \mathcal{X} = \{-1, +1\}$ and N is Gaussian with zero mean and variance σ^2. Then the following represent *equivalent* kernels:

$$l^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(z) = \frac{\mathrm{e}^{-z} \int_{-\infty}^{+\infty} \frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{(\cosh(\frac{w-z}{2}))^2} \mathrm{d}w}{\int_{-\infty}^{+\infty} \frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{(\cosh(\frac{w}{2}))^2} \mathrm{d}w}, \tag{i}$$

$$l'^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(z) = \frac{1 - \mathbb{E}[\mathbb{E}[X|Y, \Phi = z]^2]}{1 - \mathbb{E}[\mathbb{E}[X|Y]^2]}, \tag{ii}$$

$$l''^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(z) = \frac{1 - \mathbb{E}[X|Y, \Phi = z]}{1 - \mathbb{E}[X|Y]}. \tag{iii}$$

Hereby, Φ denotes a further observation of X which is conditionally independent of Y, which is the result of passing X through a symmetric channel, and which is assumed to be in log-likelihood form (if we use coding, Φ represents the extrinsic estimate of X in the L-domain).

Discussion: This lemma provides several equivalent representations of the kernel for the BAWGN channel. The expression (ii) shows the relationship between conditional entropy and mean-square error (MSE) estimator. To see this, observe first that the denominator is a (z independent) scaling factor depending on our parameterization of the channel through its entropy $\mathtt{h}$. Second, observe that the numerator $1 - \mathbb{E}[\mathbb{E}[X|Y, \Phi = z]^2] = \mathbb{E}[\mathbb{E}[X^2|Y, \Phi = z] - \mathbb{E}[X|Y, \Phi = z]^2]$ is the mean-square error estimator (which in this framework includes the decoding estimate z). This elegant relationship which connects a fundamental information theoretic quantity (the conditional entropy, or, equivalently, the mutual information) to a measure widely-used in signal processing was first observed by Guo, Shamai and Verdú in [7], [26]. In the above lemma, the channel inputs are binary. In Lemma 20 we give an alternative way of deriving $l^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(z)$ in the more general context of non-binary channel inputs.

The form (iii) provides a further simplification. This expression, in which the numerator shows the magnetization was first stated in [8] using the Nishimori identity (in the context of coding, this identity was first discussed in [28]).

Before proving Lemma 18, let us recall the following well-known fact which will be used several times in the following: Consider a BMS channel $p_{Y|X}(y|x)$ and $f(y)$, a measurable function. If $f(y)$ is even, then $\mathbb{E}_Y[f(Y)] = \mathbb{E}_{Y|X=1}[f(Y)]$.
Proof: Under the all-one assumption, the channel density is $\mathsf{c}(w) \triangleq \mathsf{c}_{\text{BAWGNC}(\mathsf{h})}(w) = \frac{\sigma}{\sqrt{8\pi}}\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}$.
(i) The kernel as stated in Lemma 3 is expressed in terms of the derivative of $\mathsf{c}(w)$ with respect to the channel parameter. To get a more pleasing analytic expression we use the fact that for the Gaussian case we can express this derivative via the identity $\frac{\partial \mathsf{c}(w)}{\partial \epsilon} = -\frac{\partial \mathsf{c}(w)}{\partial w} + \frac{\partial^2 \mathsf{c}(w)}{\partial w^2}$. Now, use the parameterization $\epsilon \triangleq 2/\sigma^2$. Then using twice integration by parts (as in [8]), we get

$$\begin{aligned} l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z)\frac{\mathrm{d}\epsilon}{\mathrm{d}\mathsf{h}} &= \int_{-\infty}^{+\infty} \frac{\partial \mathsf{c}(w)}{\partial \epsilon}\log(1+\mathrm{e}^{-w-z})\mathrm{d}w \\ &= \int_{-\infty}^{+\infty} \frac{\partial \mathsf{c}(w)}{\partial w}\frac{\mathrm{e}^{-w-z}}{1+\mathrm{e}^{-w-z}}\mathrm{d}w \\ &\quad - \int_{-\infty}^{+\infty} \mathsf{c}(w)\frac{\mathrm{e}^{-w-z}}{1+\mathrm{e}^{-w-z}}\mathrm{d}w \\ &= \int_{-\infty}^{+\infty} \mathsf{c}(w)\frac{-1}{(1+\mathrm{e}^{w+z})^2}\mathrm{d}w \\ &= \frac{-\mathrm{e}^{-z}}{4}\int_{-\infty}^{+\infty}\frac{\mathsf{c}(-w)}{(\cosh(\frac{w+z}{2}))^2}\mathrm{d}w. \end{aligned}$$

The computation of $\frac{\mathrm{d}\epsilon}{\mathrm{d}\mathsf{h}}$ is exactly the same if we set $z=0$. Therefore,

$$l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) \triangleq \frac{\mathrm{e}^{-z}\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{(\cosh(\frac{w-z}{2}))^2}\mathrm{d}w}{\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w-\epsilon)^2}{4\epsilon}}}{(\cosh(\frac{w}{2}))^2}\mathrm{d}w}.$$

(ii) First, we claim that the previous expression can be written as

$$l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) = \mathrm{e}^{-z}\frac{1-\mathbb{E}[\mathbb{E}[X|Y,\Phi=-z]^2]}{1-\mathbb{E}[\mathbb{E}[X|Y]^2]}.$$

To see this, observe that

$$\begin{aligned} w+z &\overset{(a)}{=} \log\frac{p_{\frac{2Y}{\sigma^2}|X}(w|+1)}{p_{\frac{2Y}{\sigma^2}|X}(w|-1)} + \log\frac{p_{\Phi|X}(z|+1)}{p_{\Phi|X}(z|-1)} \\ &\overset{(b)}{=} \log\frac{p_{\frac{2Y}{\sigma^2},\Phi|X}(w,z|+1)}{p_{\frac{2Y}{\sigma^2},\Phi|X}(w,z|-1)} \\ &\overset{(c)}{=} \log\frac{p_{X|\frac{2Y}{\sigma^2},\Phi}(+1|w,z)}{p_{X|\frac{2Y}{\sigma^2},\Phi}(-1|w,z)}, \end{aligned}$$

where (a) comes from the definition of w and z in Lemma 18, (b) from the independence of Y and Φ when X is given, and where (c) is the Bayes rule using $p_X(+1) = p_X(-1) = \frac{1}{2}$. Therefore,

$$\begin{aligned} \tanh(\frac{w+z}{2}) &= \frac{1-\mathrm{e}^{-w-z}}{1+\mathrm{e}^{-w-z}} \\ &= \frac{p_{X|\frac{2Y}{\sigma^2},\Phi}(+1|w,z) - p_{X|\frac{2Y}{\sigma^2},\Phi}(-1|w,z)}{p_{X|\frac{2Y}{\sigma^2},\Phi}(+1|w,z) + p_{X|\frac{2Y}{\sigma^2},\Phi}(-1|w,z)} \\ &= \mathbb{E}[X|w,z]. \end{aligned}$$

This quantity (which is often called "soft bit" as in [43]) is a bit estimate in the D-domain and the relationship $\mathbb{E}[X|w,z] = \tanh(\frac{w+z}{2})$ is in fact well-known. Therefore, since $1-(\tanh(\frac{w+z}{2}))^2 = \frac{1}{(\cosh(\frac{w+z}{2}))^2}$,

$$\begin{aligned} l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) = \mathrm{e}^{-z}&\frac{1-\int_{-\infty}^{\infty}\mathsf{c}(w)(\tanh(\frac{w+z}{2}))^2\mathrm{d}w}{1-\int_{-\infty}^{\infty}\mathsf{c}(w)(\tanh(\frac{w}{2}))^2\mathrm{d}w} \\ &\mathrm{e}^{-z}\frac{1-\mathbb{E}_{Y|X=1}[(\tanh(\frac{Y+z}{2}))^2]}{1-\mathbb{E}_{Y|X=1}[(\tanh(\frac{Y}{2}))^2]}, \end{aligned}$$

and the claim follows since, as discussed above, we can drop in the last expression the conditioning on $X=1$.

Second, as discussed in Example 4, the kernel is in general not unique in the L-domain and we can use this degree of freedom to get alternative kernels. Denote $f(z) \triangleq \frac{1-\mathbb{E}[\mathbb{E}[X_1|Y_1,-z]^2]}{1-\mathbb{E}[\mathbb{E}[X_1|Y_1]^2]}$ and observe that $l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) = \exp(-z)f(z)$ with this notation. Then, for any symmetric density $\mathsf{a}(z)$, the function $l'^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) \triangleq f(-z)$ is also a valid kernel for the L-domain since $\int_{-\infty}^{+\infty}\mathsf{a}(z)\mathrm{e}^{-z}f(z)\mathrm{d}z = \int_{-\infty}^{+\infty}\mathsf{a}(z)f(-z)\mathrm{d}z$. Therefore, an alternative kernel is

$$l'^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) = \frac{1-\mathbb{E}[\mathbb{E}[X|Y,z]^2]}{1-\mathbb{E}[\mathbb{E}[X|Y]^2]} = \frac{\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{(\cosh(\frac{w+z}{2}))^2}\mathrm{d}w}{\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{(\cosh(\frac{w}{2}))^2}\mathrm{d}w}.$$

(iii) For any symmetric random variable L, a straightforward exercise shows that $\mathbb{E}[\tanh(L/2)] = \mathbb{E}[(\tanh(L/2))^2]$. See, e.g, [8], [28]. Applied to the symmetric random variable $L \triangleq \log\frac{p(Y|+1)}{p(Y|-1)} = \frac{2}{\sigma^2}Y$ under the all-one assumption, this gives us $\mathbb{E}[\mathbb{E}[X|Y]^2] = \mathbb{E}[\tanh(\frac{L}{2})^2] = \mathbb{E}[\tanh(\frac{L}{2})] = \mathbb{E}[X|Y]$. Therefore the denominator can be easily written as $\frac{1}{1-\mathbb{E}[\mathbb{E}[X|Y]^2]} = \frac{1}{1-\mathbb{E}[X|Y]}$. We can not use directly this argument for the term $\mathbb{E}[\mathbb{E}[X|Y,z]^2] = \mathbb{E}[\tanh(\frac{Y}{\sigma^2}+\frac{z}{2})^2]$ at the numerator (the random variable $\frac{2}{\sigma^2}Y+z$ being not symmetric). However, we can look for an equivalent kernel. This is easily done by observing that the values z are provided by the symmetric random variable Φ. The sum of two symmetric random variables is again symmetric, therefore $\frac{2}{\sigma^2}Y+\Phi$ is symmetric. See, e.g., [11]. We can then use the fact that $\mathbb{E}[\tanh(L/2)] = \mathbb{E}[(\tanh(L/2))^2]$ with $L \triangleq \frac{2}{\sigma^2}Y+\Phi$ to write $\mathbb{E}_{Y,\Phi}[\mathbb{E}_X[X|Y,\Phi]^2] = \mathbb{E}_{Y,\Phi}[\mathbb{E}_X[X|Y,\Phi]]$. Therefore,

$$l''^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z) = \frac{1-\mathbb{E}[X|Y,z]}{1-\mathbb{E}[X|Y]} = \frac{\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{1+\mathrm{e}^{w+z}}\mathrm{d}w}{\int_{-\infty}^{+\infty}\frac{\mathrm{e}^{-\frac{(w\sigma^2-2)^2}{8\sigma^2}}}{1+\mathrm{e}^{w}}\mathrm{d}w}$$

is an equivalent kernel (but pointwise different from $l^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z)$ and $l'^{\mathsf{c}_{\text{BAWGNC}(\mathsf{h})}}(z)$). The last equality comes from the fact that $1-\mathbb{E}[X|Y,z] = 1-\mathbb{E}_Y[\tanh(\frac{Y+z}{2})] = \mathbb{E}_Y[\frac{2}{1+\mathrm{e}^{Y+z}}]$. ■

GEXIT and EXIT curves are in general very similar. Next lemma illuminates this fact: it shows that, in the limit of small SNR, the kernel for the BAWGNC behaves similarly to the kernel for the BSC discussed in Example 6.

Lemma 19 (Limiting Behavior of GEXIT Kernel): Consider the family $\{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}\}$ of BAWGN channels, where $\mathtt{h}$ denotes the channel entropy: The additive noise N in the model $Y = X + N$ is Gaussian with zero-mean and variance σ^2. Then

$$\lim_{\sigma\to\infty} |d|^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(s) = 1 - s^2, \quad \text{(i)}$$

$$\lim_{\sigma\to 0} |d|^{\mathsf{c}_{\text{BAWGNC}(\mathtt{h})}}(s) = 1. \quad \text{(ii)}$$

In the $|D|$-domain, the kernels are ordered between those two extremal functions.

Proof: First recall the transform formula (9) and $2\tanh^{-1}(s) = \log\frac{1+s}{1-s}$. (i) With expression (iii) of Lemma 18 we have $l^{\mathsf{c}}(2\tanh^{-1}(s)) = \frac{1-\int_{-\infty}^{+\infty}\mathsf{c}(l)\tanh(l/2+\tanh^{-1}(s))\mathrm{d}l}{1-\int_{-\infty}^{+\infty}\mathsf{c}(l)\tanh(l/2)\mathrm{d}l}$. Let us restrict ourself to the study of the term $I_\sigma(s) \triangleq \int_{-\infty}^{+\infty}\mathsf{c}(l)\tanh(l/2+\tanh^{-1}(s))\mathrm{d}l$. When $\sigma^2 \to \infty$, then the distribution of the channel inputs (more exactly of the LLR's in the L-domain) $\mathsf{c}(l) = \frac{\sigma}{2\sqrt{2\pi}}\exp(-\frac{\sigma^2(l-2/\sigma^2)^2}{8})$ becomes a Dirac centered in 0 (since its variance $4/\sigma^2 \to 0$). For any function continuous in 0, e.g., for the function $k_s : l \mapsto \tanh(l/2+\tanh^{-1}(s))$, one can indeed replace, without committing much error when $\sigma^2 \to \infty$, the integral $\int_{-\infty}^{+\infty}\mathsf{c}(l)k_s(l)\mathrm{d}l$ by $\int_{-\infty}^{+\infty}\mathsf{c}(l)k_s(0)\mathrm{d}l$. See, e.g., [44] for further details. Therefore

$$I_\sigma(z) \underset{\sigma\to\infty}{\longrightarrow} \tanh(0/2+\tanh^{-1}(s)) = s.$$

Using (9), we finally get

$$|d|^{\mathsf{c}}(s) = \frac{1-s}{2}\frac{1+s}{1} + \frac{1+s}{2}\frac{1-s}{1} = 1 - s^2.$$

(ii) The case $\sigma \to 0$ corresponds to the full knowledge of the channel input. The kernel in the $|D|$-domain converges pointwise to 1. As used for density evolution, see [11], in this case $\mathsf{c}(l)$ becomes a Dirac at ∞ a a similar argument as for (i) can be applied.

For $\epsilon \in (0,1)$, the kernels in the $|D|-$domain are ordered because of Lemma 1. ∎

As discussed before Lemma 18, the pleasing relationship presented in [7], [45] or [8] emerges for the BAWGNC. So far we have restricted ourself to the case of binary inputs. But the non-binary case as discussed in [7], [9], [45] is not much harder. This is presented in Lemma 20 using our framework.

Lemma 20 (AWGN($\mathtt{h}$)): Consider a length n code, call it $\mathtt{G}$. Assume transmission takes place over a family $\{AWGNC(\mathtt{h}_i)\}_{i\in[n]}$ where there is a global parameter ϵ such that $\mathtt{h}_i(\epsilon) = \mathtt{h}(\epsilon)$ is the entropy associated to the i^{th} channel for all $i \in [n]$. Let this parameter be $\epsilon = -2\mathsf{snr} \triangleq -\frac{2}{\sigma^2}$. Then

$$g_i(\mathtt{G},\epsilon) = \mathbb{E}\left[\mathbb{E}[X_i^2|Y] - \mathbb{E}[X_i|Y]^2\right].$$

In words, the derivative of the conditional entropy with respect to the particular paramater ϵ is equal to the Mean-Square Error (MSE) estimator.

Proof: We will prove the result in general settings when the input alphabet $\mathcal{X}$ can be any subset of $\mathbb{R}$. Temporarily, let us denote $\tilde{Y} = X + \tilde{N}$ our running Gaussian channel model. $\tilde{N}$ is the additive white Gaussian noise with zero-mean and variance σ^2. Now let us normalize this model by σ^2 to get the equivalent model $Y = \sqrt{\mathsf{snr}}X + N$ where $\mathsf{snr} = \frac{1}{\sigma^2}$ and N is an additive white Gaussian noise with zero-mean and unit-variance. In order to be a sufficient statistics, the extrinsic MAP estimate $\phi_i = \phi_i(y_{\sim i})$ can no longer be a log-likelihood ratio but, in general, a function of x_i, i.e., $\phi_i : x \mapsto \phi_i(y_{\sim i}, x)$. From (7), it follows that

$$g_i(\mathtt{G},\epsilon) = \int_{\phi_i,y_i,x_i} p(x_i)p(\phi_i \mid x_i)\frac{\mathrm{d}}{\mathrm{d}\epsilon}p(y_i|x_i)\cdot \cdot \log\left(\int_{x_i'}\frac{p(x_i'|\phi_i)p(y_i|x_i')}{p(x_i|\phi_i)p(y_i|x_i)}\mathrm{d}x_i'\right)\mathrm{d}x_i\mathrm{d}y_i\mathrm{d}\phi_i.$$

To simplify the computations, a few remarks are of order. First recall that we have chosen ϵ to be $\epsilon = -2\mathsf{snr} = \frac{-2}{\sigma^2}$. Second, observe that the Gaussian density permits us to write $\frac{\mathrm{d}p(y_i|x_i)}{\mathrm{d}\epsilon} = \frac{x_i}{\sqrt{\mathsf{snr}}}\frac{\mathrm{d}}{\mathrm{d}y_i}p(y_i|x_i)$. Therefore, integrating by parts with respect to y_i, we get

$$\begin{aligned} & g_i(\mathtt{G},\epsilon) \\ &= \int_{\phi_i,y_i,x_i} p(x_i)p(\phi_i \mid x_i)\frac{x_i}{\sqrt{\mathsf{snr}}}p(y_i|x_i)\cdot \\ &\quad \cdot \frac{\mathrm{d}}{\mathrm{d}y_i}\left\{\log\left(\int_{x_i'}\frac{p(x_i'|\phi_i)p(y_i|x_i')}{p(x_i|\phi_i)p(y_i|x_i)}\mathrm{d}x_i'\right)\right\}\mathrm{d}x_i\mathrm{d}y_i\mathrm{d}\phi_i \\ &= -\int_{\phi_i,y_i,x_i} p(x_i)p(\phi_i \mid x_i)\frac{x_i}{\sqrt{\mathsf{snr}}}p(y_i|x_i)\cdot \\ &\quad \cdot \frac{\int_{x_i'}\sqrt{\mathsf{snr}}(x_i'-x_i)p(x_i'|\phi_i)p(y_i|x_i')\mathrm{d}x_i'}{\int_{x_i'}p(x_i'|\phi_i)p(y_i|x_i')\mathrm{d}x_i'}\mathrm{d}x_i\mathrm{d}y_i\mathrm{d}\phi_i, \end{aligned}$$

after having used $\frac{\mathrm{d}p(y_i|x_i')}{\mathrm{d}y_i} = \frac{\mathrm{d}p_{Z_i}(y_i-\sqrt{\mathsf{snr}}x_i')}{\mathrm{d}y_i} = -(y_i - \sqrt{\mathsf{snr}}x_i')p(y_i|x_i')$. Let us now re-order as $p(x_i'|\phi_i)p(y_i|x_i') = p(x_i'|\phi_i,y_i)p(y_i|\phi_i)$ and use (with a slight abuse of notations) $\frac{y_i+\phi_i}{\sqrt{\mathsf{snr}}} = \mathbb{E}_{X_i}[X_i|\phi_i,y_i]$ to get

$$\begin{aligned} & g_i(\mathtt{G},\epsilon) \\ &= -\int_{\phi_i,y_i,x_i} p(x_i)p(\phi_i \mid x_i)x_i p(y_i|x_i)\cdot \\ &\quad \cdot \frac{p(y_i|\phi_i)(\frac{(y_i+\phi_i)}{\sqrt{\mathsf{snr}}}-x_i)}{p(y_i|\phi_i)}\mathrm{d}x_i\mathrm{d}y_i\mathrm{d}\phi_i \\ &= \int_{\phi_i,y_i} p(\phi_i,y_i) \\ &\quad \cdot \int_{x_i} p(x_i|y_i,\phi_i)\left(x_i^2 - \frac{(y_i+\phi_i)x_i}{\sqrt{\mathsf{snr}}}\right)\mathrm{d}x_i\mathrm{d}y_i\mathrm{d}\phi_i \\ &= \int_{\phi_i,y_i} p(\phi_i,y_i) \\ &\quad \cdot \left(\mathbb{E}_{X_i}\left[X_i^2|\phi_i,y_i\right] - \mathbb{E}_{X_i}\left[X_i|\phi_i,y_i\right]^2\right)\mathrm{d}y_i\mathrm{d}\phi_i. \end{aligned}$$

This concludes our proof since Φ_i is a sufficient statistic for $Y_{\sim i}$. ∎

APPENDIX II
PHYSICAL DEGRADATION: A CALCULUS PROOF

In this appendix we provide a direct calculus proof of Corollary 1, exploiting the explicit representation provided by Lemma 3. As a byproduct we show that the GEXIT kernel in the $|D|$-domain is non-increasing and concave. This fact is also used in the proof of Lemma 6.

For our purpose it is convenient to represent all quantities in the $|D|$-domain. Let $\{|\mathfrak{c}_{\text{BMS}(\mathfrak{h})}|\}_{\mathfrak{h}}$ denote the family of $|D|$-densities characterizing the channel family. Let $|d|^{\text{BMS}(\mathfrak{h})}(w)$ denote the GEXIT kernel in the $|D|$-domain as introduced in (9). We can rewrite it in the form

$$|d|^{\text{BMS}(\mathfrak{h})}(w) = \int_0^1 \frac{\partial|\mathfrak{c}_{\text{BMS}(\mathfrak{h})}|(z)}{\partial \mathfrak{h}} \alpha(z,w)\mathrm{d}z,$$

where

$$\alpha(z,w) = \frac{1}{4}\sum_{i,j=\pm 1}(1+iz)(1+jw)\beta(iz,jw),$$

with $\beta(z,w) = \log_2\big(1+e^{-2\tanh^{-1}(z)}e^{-2\tanh^{-1}(w)}\big)$. Finally, let $|\mathfrak{a}|$ and $|\mathfrak{b}|$ denote the two symmetric densities in the $|D|$-domain.

The claim of the theorem is then equivalent to the statement that the GEXIT functional $\int_0^1 |d|^{\text{BMS}(\mathfrak{h})}(w)|\mathfrak{a}|(w)\mathrm{d}w$ preserves the partial order implied by physical degradation. This means that if $|\mathfrak{a}| \prec |\mathfrak{b}|$ then

$$\int_0^1 |d|^{\text{BMS}(\mathfrak{h})}(w)|\mathfrak{a}|(w)\mathrm{d}w \le \int_0^1 |d|^{\text{BMS}(\mathfrak{h})}(w)|\mathfrak{b}|(w)\mathrm{d}w.$$

By Theorem 3.4 in [11], a $|D|$-domain kernel preserves the partial order implied by physical degradation if it is non-increasing and concave on $[0,1]$, i.e., if its first two derivatives are non-positive. This means we need to show that

$$\int_0^1 \frac{\partial|\mathfrak{c}_{\text{BMS}(\mathfrak{h})}|(z)}{\partial \mathfrak{h}} \frac{\partial^i \alpha(z,w)}{\partial w^i}\mathrm{d}z \le 0,$$

for $i=1,2$. By the same Theorem 3.4 the above condition is verified if both $\frac{\partial^i\alpha(z,w)}{\partial w^i}$ for $i=1,2$, are convex and non-decreasing. This in turn is true if $\frac{\partial^{i+j}\alpha(z,w)}{\partial w^i \partial z^j} \ge 0$ for $i,j=1,2$. Now some further calculus shows that

$$\begin{aligned}\frac{\partial\alpha(z,w)}{\partial w} =& \frac{1}{2}\sum_{i=\pm1} iz\log_2(1+iwz) - \\ & \frac{1}{2}\sum_{i=\pm1} i\log(1+iw),\end{aligned} \tag{22}$$

$$\ln(2)\frac{\partial^2\alpha(z,w)}{\partial w^2} = \frac{z^2}{1-w^2z^2} - \frac{1}{1-w^2}. \tag{23}$$

Note that equation (23) implies that $\frac{\partial^2\alpha(z,w)}{\partial w^2}$ has a positive expansion in z (except for the constant term). Therefore the derivatives $\frac{\partial^{2+i}\alpha(z,w)}{\partial w^2\partial z^i}$, $i=1,2$, are both positive and by symmetry of the function $\alpha(z,w)$ in its arguments z and w so is $\frac{\partial^3\alpha(z,w)}{\partial w\partial z^2}$. Finally,

$$\begin{aligned}\log(2)\frac{\partial^2\alpha(z,w)}{\partial w\partial z} &= \frac{1}{2}\ln\frac{1+wz}{1-wz} + \frac{wz}{1-w^2z^2} \\ &= 2wz\sum_{i\ge 0}\frac{(i+1)(w^2z^2)^i}{2i+1},\end{aligned}$$

which has a positive Taylor series expansion as well. This confirms our claim that the GEXIT kernel preserves the partial order implied by physical degradation.

APPENDIX III
PROOF OF EQ. (19)

In this appendix we prove the claim (19). First notice that $\mathfrak{B}(T_{\mathfrak{h}}(\mathsf{a})) = B_{\mathfrak{h}}\,\lambda(\mathfrak{B}(\rho(\mathsf{a})))$. Since $0 \le \lambda(x) \le 1$ and $\lambda'(x) \le \lambda'(1)$, we have

$$\begin{aligned}|\,\mathfrak{B}(T_{\mathfrak{h}_1}(\mathsf{a}_1)) - \mathfrak{B}(T_{\mathfrak{h}_2}(\mathsf{a}_2))| \le & \\ \lambda'(1)B_{\mathfrak{h}_1}\,|\,\mathfrak{B}(\rho(\mathsf{a}_1)) - \mathfrak{B}(\rho(\mathsf{a}_2))| + |B_{\mathfrak{h}_1} - B_{\mathfrak{h}_2}|\,.\end{aligned} \tag{24}$$

In order to estimate $|\,\mathfrak{B}(\rho(\mathsf{a}_1)) - \mathfrak{B}(\rho(\mathsf{a}_2))|$, define, for $t\in[0,1]$, $\mathsf{a}_t = (1-t)\mathsf{a}_1 + t\mathsf{a}_2$, and write

$$|\,\mathfrak{B}(\rho(\mathsf{a}_1)) - \mathfrak{B}(\rho(\mathsf{a}_2))| \le \int_0^1 \left|\frac{\mathrm{d}\,\mathfrak{B}(\rho(\mathsf{a}_t))}{\mathrm{d}t}\right|\mathrm{d}t\,. \tag{25}$$

The derivative of the Battacharyya parameter is easily computed (to lighten the notation we omit hereafter the argument of $\mathfrak{B}(\,\cdot\,)$ in the derivative). The result is most conveniently expressed in terms of densities of the variable $u \triangleq \sqrt{1-\tanh^2(x/2)}$, where x is the log-likelihood ratio (this quantity is equivalent to the $|D|$-variable and its expectation is Battacharyya parameter). If we denote the corresponding densities by the same symbols, we get

$$\begin{aligned}\frac{\mathrm{d}\,\mathfrak{B}}{\mathrm{d}t} = \rho'(1)\int_0^1 \sqrt{u_1^2+u_2^2-u_1^2u_2^2}\,\cdot & \\ \cdot\,(\mathsf{a}_2(u_1) - \mathsf{a}_1(u_1))\,\mathsf{b}(u_2)\,\mathrm{d}u_1\,\mathrm{d}u_2\,,\end{aligned} \tag{26}$$

where we introduced the density

$$\mathsf{b} \triangleq \frac{1}{\rho'(1)}\sum_{\mathtt{r}}\rho_{\mathtt{r}}(\mathtt{r}-1)\,\mathsf{a}_t^{*(\mathtt{r}-2)}\,.$$

Using integration by parts with respect to u_1 in Eq. (26) and denoting by A_1, A_2 the distributions corresponding to densities a_1, a_2, we get

$$\begin{aligned}\frac{\mathrm{d}\,\mathfrak{B}}{\mathrm{d}t} = \rho'(1)\int_0^1 \frac{u_1(1-u_2^2)}{\sqrt{u_1^2+u_2^2-u_1^2u_2^2}}\cdot & \\ \cdot\,(\mathsf{A}_2(u_1) - \mathsf{A}_1(u_1))\,\mathsf{b}(u_2)\,\mathrm{d}u_1\,\mathrm{d}u_2\,,\end{aligned}$$

Since a_2 is physically degraded with respect to a_1, $\mathsf{A}_2(u) \ge \mathsf{A}_1(u)$ for any $u\in[0,1]$. Furthermore $\int \mathsf{A}_i(v)\,\mathrm{d}v = \mathfrak{B}(\mathsf{a}_i)$. Therefore

$$\frac{\mathrm{d}\,\mathfrak{B}}{\mathrm{d}t} = \rho'(1)[\mathfrak{B}(\mathsf{a}_2) - \mathfrak{B}(\mathsf{a}_1)]\,\Xi\,, \tag{27}$$

where

$$\Xi = \int_0^1 \frac{u_1(1-u_2^2)}{\sqrt{u_1^2+u_2^2-u_1^2u_2^2}}\,f(u_1)\,\mathsf{b}(u_2)\,\mathrm{d}u_1\,\mathrm{d}u_2\,,$$

and f is a function on $[0,1]$ non negative and with unit integral. In other words, f is a probability density function. Since $\sqrt{u_1^2+u_2^2-u_1^2u_2^2} \ge u_1$, we obtain the bound

$$\begin{aligned}\Xi &\le \int_0^1 (1-u^2)\,\mathsf{b}(u)\,\mathrm{d}u \\ &= \frac{1}{\rho'(1)}\sum_{\mathtt{r}}\rho_{\mathtt{r}}(\mathtt{r}-1)\left[\int_0^1 (1-u^2)\,\mathsf{a}_t(u)\right]^{\mathtt{r}-2},\end{aligned}$$

where we used the definition of b. If we further notice that $\int_0^1 u\, \mathsf{a}_t(u) = \mathfrak{B}(\mathsf{a}_t) \geq \mathfrak{B}(\mathsf{a}_1)$, we get

$$\Xi \leq \frac{1}{\rho'(1)}\, \rho''(1 - \mathfrak{B}(\mathsf{a}_1)^2)\,. \tag{28}$$

The claim follows by putting together Eqs. (25), (27), and (28).

Appendix IV
MAP Versus BP Marginals: Some Technical Details

In this appendix we present the proofs which were omitted in Sec. X.

Proof: [Lemma 15] Let us make a few preliminary remarks. The first one follows immediately from the definition:

$$\mathbb{E}\left\{\mu_{\mathsf{Y}}(Y) \,|\, Z = z\right\} = \mu_{\mathsf{Z}}(z)\,. \tag{29}$$

In fact, using the Markov property, the left hand side can be written as $\mathbb{E}\{\mathbb{E}[X \,|\, Y] \,|\, Z = z\} = \mathbb{E}\{\mathbb{E}[X \,|\, Y, Z] \,|\, Z = z\}$ that is equal to $\mathbb{E}[X \,|\, Z = z] \equiv \mu_{\mathsf{Z}}(z)$.

The second remark is that, by elementary calculus, for any $0 \leq x_0 \leq x \leq 1$

$$k(x) \leq k(x_0) - \frac{1}{2}\, K\, (x^2 - x_0^2)\,.$$

Finally, for any random variable W, taking values in $[0, 1]$, we have (here $\mathrm{Var}(W)$ is the variance of W):

$$\mathbb{E}\, k(W) \leq k(\mathbb{E}\, W) - \frac{1}{2}\, K\, \mathrm{Var}(W)\,.$$

In fact, by Taylor expansion $k(W) \leq k(w_0) + k'(w_0)(W - w_0) - \frac{1}{2}\, K\, (W - w_0)$, for any $w_0 \in [0, 1]$. The claim is proved by taking expectation of both sides and setting $w_0 = \mathbb{E}W$.

These ingredients are put together as follows (here we use the shorthands μ_{Y} and μ_{Z} for, respectively, $\mu_{\mathsf{Y}}(Y)$ and $\mu_{\mathsf{Z}}(Z)$)

$$\begin{aligned}
\mathbb{E}[k(|\mu_{\mathsf{Y}}|)] &= \mathbb{E}\left\{\mathbb{E}[k(|\mu_{\mathsf{Y}}|)|Z]\right\} \\
&\leq \mathbb{E}\left\{k(\mathbb{E}[|\mu_{\mathsf{Y}}||Z]) - \frac{1}{2}\, K\, \mathrm{Var}(|\mu_{\mathsf{Y}}| \,|\, Z)\right\} \\
&\leq \mathbb{E}\left\{k(|\mathbb{E}[\mu_{\mathsf{Y}}|Z]|) - \frac{1}{2}\, K\, \left(\mathbb{E}[|\mu_{\mathsf{Y}}||Z]^2 - \mathbb{E}[\mu_{\mathsf{Y}}|Z]^2\right) - \right. \\
&\qquad\qquad \left. - \frac{1}{2}\, K\, \mathrm{Var}(|\mu_{\mathsf{Y}}| \,|\, Z)\right\} \\
&= \mathbb{E}\left\{k(|\mathbb{E}[\mu_{\mathsf{Y}}|Z]|) - \frac{1}{2}\, K\, \mathbb{E}[(\mu_{\mathsf{Y}} - \mathbb{E}[\mu_{\mathsf{Y}}|Z])^2|Z]\right\} \\
&= E\left\{k(|\mu_{\mathsf{Z}}|) - \frac{1}{2}\, K\, \mathbb{E}[(\mu_{\mathsf{Y}} - \mu_{\mathsf{Z}})^2|Z]\right\} \\
&= E[k(|\mu_{\mathsf{Z}}|)] - \frac{1}{2}\, K\, \mathbb{E}[(\mu_{\mathsf{Y}} - \mu_{\mathsf{Z}})^2]\,,
\end{aligned}$$

which completes the proof. ∎

Proof: [Lemma 16] We claim (and will prove later) that

$$\left|\tilde{\mu}_i^{\mathrm{BP},\ell}(Y) - \tilde{\mu}_i(Y)\right| \leq e^{|l(Y_i)|}\, \left|\mu_i^{\mathrm{BP},\ell}(Y) - \mu_i(Y)\right|\,,$$

where $l(y_i)$ is the log-likelihood associated to the channel output y_i. If we square and take expectation with respect to Y (recalling that $\mu_i^{\mathrm{BP},\ell}(Y)$, $\mu_i(Y)$ do not depend upon Y_i), we get

$$\mathbb{E}\left\{\left|\tilde{\mu}_i^{\mathrm{BP},\ell}(Y) - \tilde{\mu}_i(Y)\right|^2\right\} \leq C\, \mathbb{E}\left\{\left|\mu_i^{\mathrm{BP},\ell}(Y) - \mu_i(Y)\right|^2\right\}\,.$$

The thesis follows by summing over i.

We are left with the task of proving the first claim above. We recall that the conditional expectations can be represented in terms of extrinsic log-likelihoods as

$$\begin{aligned}
\mu_i(y) &= \tanh\left[\frac{1}{2}\phi_i(y_{\sim i})\right]\,, \\
\tilde{\mu}_i(y) &= \tanh\left[\frac{1}{2}(l(y_i) + \phi_i(y_{\sim i}))\right]\,.
\end{aligned}$$

Analogous formulae hold if we replace $\mu_i(y)$ (respectively $\tilde{\mu}_i(y)$) with $\mu_i^{\mathrm{BP},\ell}(y)$ (respectively $\tilde{\mu}_i^{\mathrm{BP},\ell}(y)$) and $\phi_i(y_{\sim i})$ with $\phi_i^{\mathrm{BP},\ell}(y_{\sim i})$. The claim follows immediately form the following calculus exercise below. ∎

Fact 1: For any $x_1, x_2, z \in \mathbb{R}$

$$|\tanh(x_1 + z) - \tanh(x_2 + z)| \leq e^{2|z|}|\tanh(x_1) - \tanh(x_2)|\,.$$

Proof: Consider, without loss of generality, $x_1 > x_2$ and $z < 0$. It is simple to realize that, for any $x \in \mathbb{R}$

$$\begin{aligned}
1 + \tanh(x + z) &\leq 1 + \tanh(x)\,, \\
1 - \tanh(x + z) &\leq e^{-2z}(1 - \tanh(x))\,.
\end{aligned}$$

The last statement follows by writing $1 + e^{2(x+z)} \geq e^{2z}(1 + e^{2x})$ and taking the inverse of both sides.

The thesis is proved by multiplying these inequalities, and integrating over $x \in [x_1, x_2]$. ∎

References

[1] C. Méasson, A. Montanari, T. Richardson, and R. Urbanke, "Life above threshold: From list decoding to area theorem and MSE," in *Proc. of the IEEE Inform. Theory Workshop*, San Antonio, Texas, October 24–29 2004.

[2] ——, "Maximum a posteriori decoding and turbo codes for general memoryless channels," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Adelaide, Sept. 2005.

[3] C. Méasson and R. Urbanke, "An upper-bound on the ML thresholds of LDPC ensembles over the BEC," in *Proc. 41th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2003.

[4] C. Méasson, A. Montanari, and R. Urbanke, "Maxwell's construction: The hidden bridge between maximum-likelihood and iterative decoding," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Chicago, 2004.

[5] ——, "Maxwell's construction: The hidden bridge between iterative and maximum a posteriori decoding," 2005, submitted to IEEE Transactions on Information Theory.

[6] D. Guo, S. Shamai, and S. Verdu, "Mutual information and conditional mean estimation in poisson channels," in *Proc. of the IEEE Inform. Theory Workshop*, San Antonio, Texas, October 24–29 2004.

[7] ——, "Mutual information and minimum mean-square error in gaussian channels," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1261–1882, Apr. 2005.

[8] N. Macris, "Correlation inequalities: a useful tool in the theory of LDPC codes," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Adelaide, Australia, Sept. 2005.

[9] D. Guo, S. Shamai, and S. Verdu, "Additive non-gaussian noise channels: Mutual information and conditional mean estimation," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Adelaide, Australia, Sept. 2005.

[10] M. Zakai, "On mutual information, likelihood-ratios and estimation error for the additive gaussian channel," 2005, submitted IEEE IT.

[11] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2005, in preparation.

[12] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[13] ——, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inform. Theory*, vol. 47, pp. 585–598, 2001.

[14] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599–618, Feb. 2001.

[15] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.

[16] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: model and erasure channel property," *IEEE Trans. Inform. Theory*, vol. 50, no. 11, pp. 2657–2673, Nov. 2004.

[17] S. ten Brink, "Convergence of iterative decoding," *Electron. Lett.*, vol. 35, no. 10, pp. 806–808, May 1999.

[18] ——, "Iterative decoding for multicode CDMA," in *Proc. IEEE VTC*, vol. 3, May 1999, pp. 1876–1880.

[19] S. ten Brink, "Designing iterative decoding schemes with the extrinsic information transfer chart," *AEU Int. J. Electron. Commun.*, vol. 54, pp. 389–398, 2000.

[20] S. ten Brink, "Iterative decoding trajectories of parallel concatenated codes," in *Proc. 3rd IEEE/ITG Conf. Source Channel Coding*, Jan. 2000, pp. 75–80.

[21] ——, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[22] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[23] I. Land, P. Hoeher, S. Huettinger, and J. B. Huber, "Bounds on information combining," in *Proc. of the 3rd Int. Symp. on Turbo Codes and Related Topics*, Brest, France, Sept. 2003.

[24] S. Huettinger and J. B. Huber, "Information processing and combining in channel coding," in *Proc. of the 3rd Int. Symp. on Turbo Codes and Related Topics*, Brest, France, Sept. 2003.

[25] I. Sutskover, S. Shamai, and J. Ziv, "Extremes of information combining," in *Proc. 41th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, 2003.

[26] D. Guo, S. Shamai, and S. Verdú, "Mutual information and MMSE in gaussian channels," in *IEEE International Symposium on Information Theory*, Chicago, USA, June 27 - July 2 2004, p. 349.

[27] A. Montanari, "The glassy phase of Gallager codes," *Eur. Phys. J. B*, vol. 23, pp. 121–136, 2001.

[28] ——, "Tight bounds for LDPC and LDGM codes under MAP decoding," *IEEE Trans. Inform. Theory*, vol. 51, no. 9, pp. 3221 – 3246, Sept. 2005.

[29] G. Wiechman and I. Sason, "Improved bounds on the parity-check density and achievable rates of binary linear block codes with applications to LDPC codes," May 2005, submitted to IEEE IT, arXiv:cond-math/cond-mat/0505057.

[30] D. Burshtein, M. Krivelevich, S. L. Litsyn, and G. Miller, "Upper bounds on the rate of LDPC codes," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2437–2449, Sept. 2002.

[31] A. N. Shiryaev, *Probability*. Springer, 1996.

[32] R. F. Brown, *A topological introduction to nonlinear analysis*. Birkhäuser, 1993.

[33] I. Land, P. Hoeher, S. Huettinger, and J. B. Huber, "Bounds on information combining," *IEEE Trans. Inform. Theory*, vol. 51, no. 2, pp. 612–619, 2005.

[34] I. Sutskover, S. Shamai, and J. Ziv, "Constrained information combining: Theory and applications for LDPC coded systems," 2005, submitted IEEE IT.

[35] K. Bhattad and K. R. Narayanan, "An MSE based transfer chart to analyze iterative decoding schemes," in *Proc. of the Allerton Conf. on Commun., Control and Computing*, Monticello, IL, USA, Oct. 2004.

[36] A. Shokrollahi, "Capacity-achieving sequences," in *Codes, Systems, and Graphical Models*, ser. IMA Volumes in Mathematics and its Applications, B. Marcus and J. Rosenthal, Eds., vol. 123. Springer-Verlag, 2000, pp. 153–166.

[37] P. Oswald and A. Shokrollahi, "Capacity achieving sequences for the erasure channel," in *Proceedings of the International Symposium on Information Theory, Washington DC*, 2001, p. 48.

[38] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: a model and two properties," in *Proc. of Conference on Information Sciences and Systems (CISS)*, Princeton University, Mar. 2002.

[39] A. Ashikhmin, G. Kramer, and S. ten Brink, "Code rate and the area under extrinsic information transfer curves," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Lausanne, Switzerland, June 30–July 5 2002, p. 115.

[40] C. Méasson and R. Urbanke, "Asymptotic analysis of turbo codes over the binary erasure channel," in *Proc. of the 12th Joint Conference on Communications and Coding*, Saas Fee, Switzerland, March 2002.

[41] ——, "Further analytic properties of EXIT-like curves and applications," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Yokohama, Japan, June 29–July 4 2003, p. 266.

[42] G. D. Forney, "Lecture notes," 2005, mIT.

[43] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 429–445, Mar. 1996.

[44] A. H. Zemanian, *Distribution Theory and Transform Analysis*. New York, USA: Dover Publications, 1965.

[45] D. Guo, "Gaussian channels: Information, estimation and multiuser detection," Ph.D. dissertation, Princeton University, 2004.