Probabilistic Parity Shaping for Linear Codes

Georg Böcherer, Member, IEEE, Diego Lentner, Alessandro Cirino, Fabian Steiner, Student Member, IEEE

Abstract—Linear layered probabilistic shaping (LLPS) is proposed, an architecture for linear codes to efficiently encode to shaped code words. In the previously proposed probabilistic amplitude shaping (PAS) architecture, a distribution matcher (DM) maps information bits to shaped bits, which are then systematically encoded by appending uniformly distributed parity bits. LLPS extends PAS by probabilistic parity shaping (PPS), which uses a syndrome DM to calculate shaped parity bits. LLPS enables the transmission with any desired distribution using linear codes, furthermore, by LLPS, a given linear code with rate $R_{\text{fec}}$ can be operated at any rate $R \leq R_{\text{fec}}$ by changing the distribution. LLPS is used with an LDPC code for dirty paper coding against an interfering BPSK signal, improving the energy efficiency by 0.8 dB.

I. INTRODUCTION

Communication channels often have non-uniform capacity-achieving input distributions, which has been the main motivation for probabilistic shaping (PS), i.e., the development of practical transmission schemes that use non-uniform input distributions. Many different PS schemes have been proposed in literature, see, e.g., the literature review in [1] Sec. II. Probabilistic amplitude shaping (PAS) [1] uses distribution matching (DM) to map information bits to shaped bits, which are then systematically encoded to append uniformly distributed parity bits. PAS integrates with any linear forward error correction (FEC) code. For higher-order modulation for the additive white Gaussian noise (AWGN) channel, PAS is capacity-achieving [2] Sec. 10.3,[3] and has found wide applications for optical [4], wired [5], and wireless [6] transmission.

However, there are important cases where optimal transmission requires shaped parities [4] Remark 3], examples include intensity modulation [7] and on-off-keying (OOK). A time-sharing based shaping scheme (sparse-dense-transmission) for OOK was presented in [8], while an implementation for polar codes is shown in [9].

The layered PS random code ensemble introduced in [10], [2], [4] suggests that encoding to shaped parities is indeed possible, in particular, it suggests that for linear codes of length $n$, dimension $k$, and rate $R_{\text{fec}} = k/n$, we can encode to code words with distribution $P_B$ at rate $R = [\mathbb{H}(B) - (1 - R_{\text{fec}})]^+$ (1)

where $\mathbb{H}(B)$ denotes the entropy of $B$. However, no efficient encoding algorithm is known, see e.g., [2],[4] Remark 3], which means that encoding has to be done by a lookup table (LUT) with $2^{Rn}$ entries [4 Sec. II-E], which is prohibitively large already for short codes.

Contribution: In this work, we suggest linear layered probabilistic shaping (LLPS), which extends PAS by probabilistic parity shaping (PPS), which can be realized by a syndrome distribution matcher (SDM). For any binary linear code of length $n$ and dimension $k$, the SDM can be realized by calculating online a set of size $2^\ell$, where

$$\ell \approx (n - k) \left( \frac{1}{\mathbb{H}(B)} - 1 \right)$$ (2)

or by calculating offline a LUT of size $2^{n-k}$. The numbers $\ell$ and $n - k$ can be much smaller than $Rn$.

We apply LLPS to coding against an interfering binary phase shift keying (BPSK) signal that is known in advance to the transmitter but not to the receiver. This is an instance of the class of channels considered by Gelfand and Pinsker in [11], for which transmission schemes are often called dirty paper coding (DPC), following [12]. For an $n \approx 1000$ rate $1/2$ low-density parity-check (LDPC) code, DPC by LLPS improves the energy efficiency by 0.8 dB, with $\ell = 16$. Compared to a naive layered PS, the size of the required LUT is reduced from $2^{nR} \approx 2^{500}$ to $2^{16}$, which is significantly smaller.

Outline: In Sec. II we briefly review systematic encoding, layered PS, and PAS. We introduce LLPS in Sec. III. We then apply LLPS to DPC in Sec. IV and present numerical results. We conclude in Sec. V pointing out future research directions. Notation: We denote random variables by capital letters, e.g., $X, Y$. We denote by $\mathbb{H}(X)$ and $\mathbb{H}(X|Y)$ the entropy of $X$ and $X$ conditioned on $Y$, respectively. $I(X; Y)$ denotes the mutual information of $X$ and $Y$.

II. PRELIMINARIES

A. Systematic Encoding

Consider an $(n, k)$ binary linear code $C$ with block length $n$ and dimension $k$ and define $m = n - k$. We represent the code by an $m \times n$ parity check matrix $H$, i.e.,

$$C = \{ c \in \{0, 1\}^n : cH^T = 0 \}. \quad (3)$$

The code rate is $R_{\text{fec}} = \frac{k}{n}$. Suppose that $H$ decomposes as

$$H = [H_s | H_p] \quad (4)$$

where $H_s = m \times k$ and $H_p = m \times m$ and has full rank. Then a length $k$ vector $v$ can be systematically encoded into the codeword $[v | p]$ in two steps

1) Calculate the syndrome $s = vH_s^T$.
2) Calculate the parity bits $p = s(H_p^T)^{-1}$.

Note that

$$[v | p]H^T = vH_s^T + pH_p^T = s + s = 0 \quad (5)$$

that is, by (3), $[v | p]$ is indeed a codeword.
Combining (9) and (10), we get after some manipulations

$$R = R_{\text{f}} \mathbb{H}(V; Y) + (1 - R_{\text{f}}) \mathbb{H}(U; Y).$$

(11)

We see that the time sharing realized by PAS between shaped and unshaped channel inputs results in a time sharing achievable rate, which is in general suboptimal, by the concavity of mutual information in input distributions [14] Theorem 2.7.4.

### III. Probabilistic Parity Shaping

We now develop PPS, extending PAS by shaped parity bits.

#### A. Modified Systematic Encoding

Consider Fig. 1 and Fig. 2. As in Sec. II-A, we consider an $(n, k)$ binary linear code with a $m \times n$ check matrix. We again partition the check matrix into $H = [H_u | H_p]$, however, we modify the size of $H_u$ and $H_p$ to $m \times (k - \ell)$ and $m \times (m + \ell)$, respectively. The systematic encoding is as follows:

1) For length $k - \ell$ vector $v$, calculate the syndrome $s = vH_u^T$.

2) Calculate $m + \ell$ parity bits $p$ by solving

$$p: pH_p^T = s.$$  

(12)

Since $H_p$ is $m \times (m + \ell)$, the condition $pH_p^T = s$ is fulfilled by many different solutions $p$, consequently, we can choose the parity bits $p$ subject to a shaping constraint. This is realized by an SDM, which we discuss in more detail next.

#### B. Linear Codes and Shaping

Consider a memoryless binary input channel $P_{\text{Y}|\text{B}}$. By [10], correct decoding is possible if the overhead $1 - R_{\text{f}}$ fulfills

$$1 - R_{\text{f}} > \mathbb{H}(B|Y).$$

(6)

To relate code parameters to information measures, we consider (hypothetical) ideal codes with $1 - R_{\text{f}} = \mathbb{H}(B|Y)$. The number of check equations of an ideal linear code is then given by

$$m = n - k = n(1 - R_{\text{f}})$$

(7)

$$= n \mathbb{H}(B|Y).$$

(8)

#### C. PAS

In PAS (see Fig. 3), length $k_{\text{info}} \leq k$ information bits $u$ are mapped by a DM to $k$ shaped bits $v$ following the distribution $P_v$. The shaped bits $v$ are then systematically encoded to the codeword $[v|p]$, as described in Sec. II-A. Consequently, the transmitted codeword has $k$ shaped bits $v$ and $m$ unshaped parity bits $p$ with the uniform distribution $P_U$. In higher-order modulation, the partially shaped codeword can be used for optimal signaling by using the shaped bits to address amplitudes and the unshaped bits to address signs [11].

The number of check equations $m$ of an ideal code is equal to the average uncertainty of PAS, i.e.,

$$m = n \mathbb{H}(V|Y) + (1 - R_{\text{f}}) \mathbb{H}(U|Y).$$

(9)

By [13], the ideal DM has rate $\mathbb{H}(V)$, so that

$$R = \frac{k_{\text{info}}}{n} = \frac{\mathbb{H}(V)k}{n} = \mathbb{H}(V)R_{\text{f}}.$$  

(10)
C. Rate Matching by LLPS

Suppose we use LLPS to encode into code words with distribution \( P_B \). We realize the SDM by using as cost function the cross entropy

\[
 f(p) = \frac{1}{m + \ell} \sum_{i=1}^{m+\ell} \log_2 \frac{1}{P_B(p_i)}. \tag{19}
\]

The ideal FEC code has \( 1 - R_{\text{tec}} = \mathbb{H}(V|Y) \), the ideal DM has rate \( k_{\text{info}}/(k-\ell) = \mathbb{H}(B) \), and the ideal SDM has rate \( m/(m+\ell) = \mathbb{H}(B) \), which translates into the following equations

\[
 m = n \mathbb{H}(B|Y) \tag{20}
\]

\[
 k_{\text{info}} = \mathbb{H}(B)(k-\ell) \tag{21}
\]

\[
 m = \mathbb{H}(B)(m+\ell). \tag{22}
\]

We now have

\[
 R = \frac{k_{\text{info}}}{n} = \frac{\mathbb{H}(B)(k-\ell)}{n} \tag{23}
\]

\[
 = \frac{\mathbb{H}(B)(k+m-m-\ell)}{n} \tag{24}
\]

\[
 = \frac{\mathbb{H}(B) - \mathbb{H}(B|(m+\ell)}{n} \tag{25}
\]

\[
 = \frac{\mathbb{H}(B) - \mathbb{H}(B|Y) = \mathbb{I}(B;Y)}. \tag{26}
\]

We conclude that LLPS can operate at any rate between 0 (for \( \mathbb{H}(V) = 0 \)) and \( R_{\text{tec}} \) (for \( \mathbb{H}(V) = 1 \)), and with ideal components, LLPS achieves the optimal achievable rate \( \mathbb{I}(B;Y) \).

D. LLPS Decoding

The FEC decoder calculates its decision \( \hat{v}|\hat{p} \) from the information it is provided by demapper. Since the transmitted \( [v|p] \) is a code word, no change of the decoder is required. The decoder throws away the parity bits \( \hat{p} \) and outputs the decision \( \hat{v} \). For this, the only information required by the decoder is the value of \( \ell \).

IV. DIRTY PAPER CODING

We now apply LLPS to a dirty paper coding scenario, where SDMs with small \( \ell \), i.e., small computational cost, are sufficient to significantly improve the energy efficiency.

A. Channel Setup

We consider the scenario in Fig. 4. A binary sequence \( b^n \) (not shown in Fig. 4) is mapped to a BPSK signal \( x^n \), which is transmitted. The received signal \( y^n \) is the sum of the transmitted signal \( x^n \), an interfering BPSK signal \( z^n \), and Gaussian noise \( w^n \). The interfering signal \( z^n \) is non-causally known to the transmitter, i.e., the binary sequence \( b^n \) mapped to the transmitted signal \( x^n \) is a function of the message \( u \) and the interfering signal \( z^n \). At time instance \( i \), we have

\[
 Y_i = \alpha x_{b_i} + \beta Z_i + W_i \tag{28}
\]

where \( W_i, i = 1, \ldots, n \) are independent and zero mean Gaussian with variance \( \sigma^2 \), where \( z \) take values in \( \{-1, 1\} \), and where \( x_0 = -1 \) and \( x_1 = +1 \). The interference is uniformly distributed, i.e., \( P_Z(-1) = P_Z(1) = \frac{1}{2} \). We define the signal-to-noise-ratio (SNR) by \( 10 \log_{10}(\sigma^2/\alpha^2) \) dB and we specify the strength of the interfering signal by \( 10 \log_{10}(\beta^2/\alpha^2) \) dB.

B. Reference Strategy: Interference as Noise

The transmitter ignores the presence of \( z^n \) and the receiver treats the interfering signal as noise. The achievable rate for this reference strategy is

\[
 R = \mathbb{I}(B;Y) \tag{29}
\]

\[
 B \text{ and } Z \text{ independent, } B \text{ uniformly distributed.} \tag{30}
\]

The demapper calculates the log-likelihood ratios (LLRs)

\[
 L(y) = \log \frac{p_{Y|B}(y|0)}{p_{Y|B}(y|1)} \tag{31}
\]

where

\[
 p_{Y|B}(y|b) = \frac{1}{2} [p_W(y - \alpha x_b + \beta) + p_W(y - \alpha x_b - \beta)]. \tag{32}
\]

C. DPC

Using DPC (see, e.g., [15 Ch. 6]) we can achieve the rate

\[
 R_{\text{dpc}} = \mathbb{I}(B;Y) - \mathbb{I}(B;Z), \quad BZ \sim P_Z P_{B|Z} \tag{33}
\]

by transmitting \( B \) according to \( P_{B|Z} \). The demapper calculates the LLR

\[
 p_{Y|B}(y|b)P_{B|Z}(b) = \sum_{z \in \{-1, 1\}} p_{Y|B|Z}(y|bz)P_{B|Z}(bz) \tag{34}
\]

\[
 = \sum_{z \in \{-1, 1\}} p_{Y|B|Z}(y|bz)P_{B|Z}(b|z) \frac{1}{2} \tag{35}
\]

\[
 = \sum_{z \in \{-1, 1\}} p_W(y - \alpha x_b - \beta z)P_{B|Z}(b|z) \frac{1}{2}. \tag{36}
\]

Remark 1. We are considering the fixed bit-mapper \( B \mapsto x_B \) with \( x_0 = -1 \) and \( x_1 = +1 \). By [15 Ch. 6], [16], in some cases, the DPC achievable rate \( R_{\text{dpc}} \) can be further improved by using a time variant bit-mapper that depends on \( z_i \).

D. LLPS DPC Encoder

In Fig. 6 we display the LLPS for dirty paper coding. The DM for the systematic part \( v \) is instantiated by a SDM with matrix \( H_v \), with an identity matrix to the right and entries at the left picked uniformly at random. Both SDMs get provided the corresponding part of the interfering signal. In Fig. 5 we display the distributions that we obtained from optimizing (32), see Sec. [IVF]. The figure suggests that the...
Furthermore, we know that an ideal SDM has rate $H(B|Z)$. Thus, the rate of the DPC transmitter is
\[
\frac{H(B|Z)(k-\ell)}{n} = \frac{H(B|Z) - H(B|Z)(n-k+\ell)}{n}
\]
(40)
\[
= \frac{H(B|Z) - n-k}{n}
\]
(41)
\[
= H(B|Z) - H(B|Y)
\]
(42)
\[
= I(B;Y) - I(B;Z)
\]
(43)
which recovers the achievable rate (32).

E. Ideal LLPS Rate

By (7), we know that the ideal FEC code has redundancy
\[
m = n - k = H(B|Y)n.
\]
(39)
Furthermore, we know that an ideal SDM has rate $H(B|Z)$. The employed non-uniform distribution
\[
P_{B|Z} = \begin{bmatrix} P_{B|Z}(0\mid0) & P_{B|Z}(0\mid1) \\ P_{B|Z}(1\mid0) & P_{B|Z}(1\mid1) \end{bmatrix} = \begin{bmatrix} 0.6037 & 0.3963 \\ 0.3963 & 0.6037 \end{bmatrix}
\]
(44)
The outer SDM has rate $k_{\text{info}}/(k - \ell) = 496/(528 - 16) = 0.9688$ bits, and the inner SDM has rate $m/(m + \ell) = 0.9706$ bits. One hundred belief propagation iterations are performed. We observe gains of about 0.8 dB in Fig. 8 recovering the asymptotic gain suggested by Fig. 7.

V. CONCLUSIONS

We proposed a linear layered probabilistic shaping (LLPS) architecture that extends PAS by probabilistic parity shaping
(PPS). LLPS integrates with any linear FEC and enables shaped parity bits, which are required, e.g., for optimized OOK. LLPS is a promising architecture for the probabilistic shaping problems considered in [7], [8], [4, Remark 3]. The enabling component of LLPS is a syndrome DM (SDM) defined on a \( m \times (m + \ell) \) check matrix \( H_p \), which maps a syndrome to the vector in the corresponding coset that minimizes a cost function. LLPS was applied to a dirty paper coding problem, improving the energy efficiency by 0.8 dB. Future research should develop SDM algorithms that work efficiently also when neither \( m \) nor \( \ell \) are small.

References

[1] G. Böcherer, F. Steiner, and P. Schulte, “Bandwidth efficient and rate-matched low-density parity-check coded modulation,” IEEE Trans. Commun., vol. 63, no. 12, pp. 4651–4665, Dec. 2015.
[2] G. Böcherer, “Principles of coded modulation,” Habilitation thesis, Technical University of Munich, 2018. [Online]. Available: http://www.georg-boecherer.de/bocherer2018principles.pdf
[3] R. A. Amjad, “Information rates and error exponents for probabilistic amplitude shaping,” in Proc. IEEE Inf. Theory Workshop (ITW), Guangzhou, China, Nov. 2018.
[4] G. Böcherer, P. Schulte, and F. Steiner, “Probabilistic Shaping and Forward Error Correction for Fiber-Optic Communication Systems,” J. Lightw. Technol., vol. 37, no. 2, pp. 230–244, Jan. 2019.
[5] P. Iannone, Y. Lefevre, W. Coomans, D. van Veen, and J. Cho, “Increasing cable bandwidth through probabilistic constellation shaping,” in Proc. SCTE-ISBE, 2018.
[6] Y. C. Gultekin, W. J. van Houtum, S. Şerbetli, and F. M. Willems, “Constellation shaping for IEEE 802.11,” in Proc. IEEE Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC), 2017.
[7] T. A. Eriksson, M. Chapron, F. Buchali, K. Schuh, S. ten Brink, and L. Schmalen, “56 Gbaud probabilistically shaped PAM8 for data center interconnects,” in Proc. Eur. Conf. Optical Commun. (ECOC), 2017.
[8] A. Git, B. Matuz, and F. Steiner, “Protograph-Based LDPC Code Design for Probabilistic Shaping with On-Off Keying,” in Proc. Ann. Conf. Inf. Sci. Syst. (CISS), Mar. 2019.
[9] T. Wiegart, F. Steiner, and P. Yuan, “Shaped On-Off-Keying Transmission Using Polar Codes,” Mar. 2019, in preparation.
[10] G. Böcherer, “Achievable rates for probabilistic shaping,” arXiv preprint, 2017. [Online]. Available: https://arxiv.org/abs/1707.01134v5
[11] I. G. Gelfand and M. S. Pinkser, “Coding for channels with random parameters,” Prob. Contr. Inf. Theory, vol. 9, no. 1, pp. 19–31, 1980.
[12] M. Costa, “Writing on dirty paper,” IEEE Trans. Inf. Theory, vol. 64, no. 2, pp. 439–441, May 1982.
[13] P. Schulte and G. Böcherer, “Constant composition distribution matching,” IEEE Trans. Inf. Theory, vol. 62, no. 1, pp. 430–434, Jan. 2016.
[14] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. John Wiley & Sons, Inc., 2006.
[15] G. Kramer, “Topics in multi-user information theory,” Foundations and Trends in Comm. and Inf. Theory, vol. 4, no. 4–5, pp. 265–444, 2007.
[16] D. Lentner, “Dirty paper coding for higher-order modulation and finite constellation interference,” Master’s thesis, Technical University of Munich, 2018.
[17] “IEEE Standard for Local and Metropolitan Area Networks Part 16,” 2006.