Hybrid Vector Perturbation Precoding: The Blessing of Approximate Message Passing

Shanxiang Lyu and Cong Ling, Member, IEEE

Abstract—Vector perturbation (VP) precoding is a promising technique for multiuser communication systems operating in the downlink. In this work, we introduce a hybrid framework to improve the performance of lattice reduction (LR) aided (LRA) VP. Firstly, we perform a simple precoding using zero forcing (ZF) or successive interference cancellation (SIC) based on a reduced lattice basis. Since the signal space after LR-ZF or LR-SIC precoding can be shown to be bounded to a small range, then along with sufficient orthogonality of the lattice basis guaranteed by LR, they collectively pave the way for the subsequent application of an approximate message passing (AMP) algorithm, which further boosts the performance of any suboptimal precoder. Our work shows that the AMP algorithm in compressed sensing can be beneficial for a lattice decoding problem whose signal constraint lies in \( \mathbb{Z} \) and entries of the input lattice basis not necessarily being i.i.d. Gaussian. Numerical results show that the developed hybrid scheme can provide performance enhancement with negligible increase in the complexity.

Index Terms—Vector perturbation, lattice reduction, approximate message passing

I. INTRODUCTION

The broadband mobile internet of the next generation is expected to deliver high volume data to a large number of users simultaneously. To meet this demand in the broadcast network, it is desirable to precode the transmit symbols according to the channel state information (CSI) with improved time-efficiency while retaining the reliability. It has been indicated that plain channel inversion performs poorly at all signal-to-noise ratios (SNRs), and further regularization cannot improve the performance substantially. In [1], [2], the authors proposed a precoding scheme called vector perturbation (VP) based on Tomlinson-Harashima precoding to modify the transmitted data by modulo-lattice operations, and the scheme has been shown to be achieving near-sum-capacity of the system, which does not require explicit dirty-paper techniques.

The optimization target in a VP problem represents a closest vector problem (CVP) in a lattice perspective, which has been proved NP-complete by a reduction from the decision version of CVP [3]. Therefore, the sphere decoding technique [4] adopted in [1], [2] (referred to as sphere precoding) is computationally prohibitive for large-scale systems. This hardness especially looms in the VP precoding problem because there is no prior on the distance from a target to the lattice, and the lattice bases in VP are not Gaussian random, so that Hassibi’s expected complexity analysis [5] no longer suits this setting. The complexity issue is indeed one of the three main challenges associated with VP, where the other two issues are about its power scaling factor and large signal space [6], [7].

To bypass the complexity issue of sphere precoding, much work has been done in recent years to explore low complexity CVP algorithms in multiuser (MU) multiple-input multiple-output (MIMO) communications, e.g., cf. [6], [8], [9], [10], [11], [12], [13]. The spirit of these results is to address CVP on a sub-lattice or impose a constraint for the signal space of sphere precoding. E.g., in [11], the authors proposed to alternatively solve a CVP about a selective sub-basis of a smaller dimension, whose associated complexity of VP depends on the size of the new basis. As for the sparse vector perturbation technique in [13], it also belongs to the class of selective vector perturbation where it only selects two vectors. The reduction on the target vector in [13] is then applied to all basis vectors sequentially, which resembles a special case of the sequential lattice reduction [14]. There is however no theoretical performance guarantee for these simplified methods, so we have to resort to a lattice reduction (LR) aided (LRA) precoding scheme [10], [15], [16], which had been shown diversity achieving [16]. In addition to their theoretical guarantees, LRA methods particularly suit slow fading channels, where the lattice basis is fixed during a large number of time slots and only the CVP targets are changing.

We investigate VP by using LRA methods in this work. LR has become quite popular in both MIMO precoding and decoding, especially after the pioneering work of Lenstra–Lenstra–Lovász (LLL) [17]. In recent years, in addition to the polynomial LLL algorithm, more researchers are showing interests in strong lattice reduction algorithms such as Minkowski’s reduction [18], [19], Korkine-Zolotarev’s (KZ) reduction [20] and its boosted version [21]. The performance of LRA precoding is not well understood except [10], [16], so our primary motivation is to investigate how far LRA methods can go, especially with the blessing of algorithms from compressed sensing.

We propose to use a message passing algorithm to explore the vicinity of sub-optimal solutions under the LRA framework. The approximate message passing (AMP) algorithm was initially proposed by Donoho, Montanari and Maleki in [22]. [23], [24] to solve the least-absolute shrinkage and selection operator (Lasso) problem in compressed sensing, which has much lower complexity than previous benchmark algorithms. Researchers have been adopting message passing algorithms to solve problems in MIMO detection [25], [26], [27] with small constellation sizes, where the assumed Rayleigh fading channel assists to model the input lattice basis with i.i.d. Gaussian entries. It is noteworthy that directly applying AMP
in MIMO detection problems cannot be diversity achieving because a general discrete prior renders the AMP threshold function not Lipschitz continuous in high signal-to-noise-ratio (SNR), so channel coding is often required (e.g., cf. [25]). If we want to embrace the low complexity advantage of AMP, several practical issues must be hampered. i) the lattice basis in VP is not a Gaussian random one nor its dual, while [28] shows the entries have to be at least sub-Gaussian and the generalized AMP (GAMP) [29], [30] only shows convergence of the algorithm with the aid of damping. ii) the problem size may not be infinitely large, and we should make AMP feasible in the non-asymptotic region (say, the base station is equipped with 20 antennas to serve 20 users). iii) the constellation in AMP cannot be integers. Fortunately, AMP in conjunction with a reduced lattice basis can alleviate all these concerns.

The contributions of this paper are summarized as twofold:

1) After showing boosted LLL/KZ (b-LLL/b-KZ) reduced bases are good for AMP, we analyze the energy efficiency of LRA precoding with zero-forcing (ZF) or successive-interference-cancellation (SIC) precoding. b-LLL/b-KZ suits compressed sensing scenarios because they yield bases with small coherence parameters, and an orthogonality metric in lattice theory is indeed reflecting the same goodness. The proved bound on LR-ZF/SIC not only shows that a sub-optimal estimator has a power scaling factor not far from that of sphere precoding, but also reveals that we can subtract the LR-ZF/SIC estimation to get into another estimation problem of a bounded constellation size. Since the bound on constellation size is derived from a worst case analysis, we also empirically shows a small constellation size suffices for our new problem.

2) For the first time, the AMP algorithm is successfully deployed to address a lattice decoding problem with an arbitrary input basis and an integer prior Z. A reduced lattice basis may still not suit the basis assumption of AMP, so we derive a new one based on the exposition of Montanari [24] and Maleki [31]. This derivation can be associated with a state evolution equation, where the impacts of lattice reduction and parameter selections are revealed explicitly. We propose to impose a ternary prior for AMP, so that the threshold functions have closed forms and the whole algorithm has relatively low complexity. This design helps to explore all the 3^n adjacent Voronoi cells of a LR-SIC/ZF one. Numerical results show that we can get a few dB’s gain after concatenating AMP to previous LRA-ZF/SIC.

The rest of this paper is organized as follows. We review some basic concepts about lattices and VP in Sec. II. The hybrid scheme is explained in Sec. III which includes demonstrations about why we have reached another problem with a finite constellation size. Sec. IV presents our AMP algorithm. And lastly we give out simulation results and conclusions.

Notation: Matrices and column vectors are denoted by uppercase and lowercase boldface letters. ⌊·⌋ denotes rounding, ⌈·⌉ denotes the absolute value, ∥·∥ denotes the Euclidean norm, and † stands for pseudoinverse. span(S) denotes the vector space spanned by S. πS(x) and πS(x) denote the projection of x onto span(S) and the orthogonal complement of span(S). ≈ stands for equality up to a normalization constant. [n] denotes {1, ..., n}, (x) = ∑n i=1 x_i/n. In the message passing algorithms, we take {a, b}, {i, j} to index the rows and columns of H, respectively. We use the standard asymptotic notation p(x) = O(q(x)) when lim sup_{x→∞} |p(x)/q(x)| < ∞.

II. PRELIMINARIES

A. Lattices

An n-dimensional lattice is a discrete additive subgroup in \( \mathbb{R}^n \). A Z-lattice with basis \( H = [h_1, ..., h_n] \in \mathbb{R}^{m \times n} \) can be represented by

\[
L(H) = \left\{ v \mid v = \sum_{i \in [n]} c_i h_i, \ c_i \in \mathbb{Z} \right\}.
\]

The ith successive minimum of \( L(H) \) is the smallest real number \( r \) such that \( L(H) \) contains \( i \) linearly independent vectors of length at most \( r \):

\[
\lambda_i(H) = \inf \left\{ r \mid \dim(\text{span}(L \cap B(0, r))) \geq i \right\},
\]

in which \( B(t, r) \) denotes a ball centered at \( t \) with radius \( r \).

It is necessary to distinguish whether a lattice basis is good or not. Good means all the lattice vectors are short and nearly orthogonal, and this property is measured by the orthogonality defect (OD):

\[
\xi(H) = \frac{\prod_{i=1}^n \|h_i\|}{\sqrt{\det(H^T H)}}.
\]  

We have \( \xi(H) \geq 1 \) due to Hadamard’s inequality.

Lattice reduction is the process to transform a bad lattice basis into a good one. Depending on what type of goodness we are pursuing, and how much complexity we can afford, there are many well developed reduction algorithms. Here we review the polynomial time LLL [17] reduction and the exponential time KZ [20] reduction because most reduction algorithms can be interpreted as variants of these two.

We shall present the definitions of LLL/KZ reduction, whose algorithmic routines can be found in [32]. Let \( R \) be the R matrix of a QR decomposition on \( H \), with elements \( r_{i,j} \)’s, and \( \delta \in (1/4, 1] \) be a Lovász constant.

Definition 1 ([17]). A basis \( H \) is called LLL reduced if it satisfies the size reduction conditions of \( |r_{i,j}/r_{i,i}| \leq \frac{1}{2} \) for \( 1 \leq i \leq n, j > i \), and Lovász conditions of \( \delta r_{i,i}^2 \leq r_{i,i+1}^2 + r_{i+1,i+1}^2 \) for \( 1 \leq i \leq n - 1 \).

Define \( \beta = 1/\sqrt{\delta - 1/4} \in (2/\sqrt{3}, \infty) \). If \( H \) is LLL reduced, it has [17]

\[
\xi(H) \leq \beta^{n(n-1)/2}.
\]  

Definition 2 ([33]). A basis \( H \) is called KZ reduced if it satisfies the size reduction conditions, and the projection conditions of \( \pi_{[h_1, ..., h_{i-1}]}(h_i) \) being the shortest vector of the projected lattice \( L_{[h_1, ..., h_{i-1}]}([h_1, ..., h_n]) \) for \( 1 \leq i \leq n \).

If \( H \) is KZ reduced, it has [33]

\[
\xi(H) \leq \left( \prod_{i=1}^n \sqrt{\frac{i+3}{2}} \right) \left( \frac{2n}{3} \right)^{n/2}.
\]  

It has been shown in [21] that the boosted version of LLL/KZ can produce shorter and more orthogonal basis vectors.
Definition 3 (21). A basis $H$ is called boosted LLL (b-LLL) reduced if it satisfies diagonal reduction conditions of $\delta_{i,i}^2 \leq (r_{i,i+1} - |r_{i,i+1} / r_{i,i}| r_{i,i})^2 + r_{i+1,i+1}^2$ for $1 \leq i \leq n-1$, and all $h_i$ for $2 \leq i \leq n$ are reduced by an approximate CVP oracle with list size $L$ along with a rejection operation.

Although the definition of b-LLL ensures that it performs no worse than LLL, only the same bound on OD has been proved: $\xi(H) \leq 2^{n(n-1)/2}$ (21).

Definition 4 (21). A basis $H$ is called boosted KZ (b-KZ) reduced if it satisfies the projection conditions as KZ, and the length reduction conditions of $\|h_i\| \leq \|h_1 - Q(\pi_2(h_1,\ldots,h_{i-1})(\pi_1(h_1,\ldots,h_{i-1})h_i))]\|/2$ for $2 \leq i \leq n$, where $Q(\cdot)$ is a lattice quantizer.

If $H$ is b-KZ reduced, it has

$$\xi(H) \leq \sqrt{n} \left( \prod_{i=1}^{n-1} \frac{\sqrt{2} + 3}{2} \right) \left( \frac{2n}{3} \right)^{n/2}. \quad (4)$$

B. Vector Perturbation and Optimization

Vector perturbation is a precoding technique that aims to minimize the transmitted power that is associated with the transmission of a certain data vector (1. 2). Assume the MIMO system is equipped with $m$ transmit antennas and $n$ individual users, and each user has only one receive antenna. The observed signal $l$ at users 1 to $n$ can be collectively expressed as

$$l = Bt + w \quad (5)$$

where $B \in \mathbb{R}^{n \times m}$ denotes a channel matrix whose entries admit $N(0, 1)$, $t \in \mathbb{R}^m$ is a transmitted signal, and $w \sim N(0, \sigma_w^2 I_n)$ is an additive Gaussian noise.

With perfect channel knowledge at transmitter’s side, the transmitted signal $t$ is designed to be a truncation of the channel inversion precoding $B^\dagger$'s:

$$t = B^\dagger(s - Ax), \quad (6)$$

where $x \in \mathbb{Z}^n$ is an integer vector to be optimized, $s \in \mathcal{A}^n$ is the symbol vector. We set $\mathcal{A} = \{0, \ldots, A - 1\}$, because any quadrature amplitude modulation (QAM) constellation can be transformed to this format after adjusting (8), which means $A$ has an equivalent QAM size of $A^2$.

Assume the transmitted signal has unit power, and $E_t \triangleq \|t\|$ is a normalization factor. Then the received data at users can be represented as

$$l = (s - Ax) / E_t + w. \quad (7)$$

Let $l' = E_t l$, $w' = E_t w$, since $Ax$ mod $A = 0$, the receive equation can be transformed to

$$[l'] \mod A = [s + w'] \mod A. \quad (8)$$

From (8), we can see that $\|w'_i\| < \frac{A}{2} \forall i$, where $w' \in N(0, \sigma_w^2 E_t I_n)$, then $s$ can be faithfully recovered.

To decrease the decoding error probability which is dominated by $E_t$, we have to address the following optimization problem at the transmitter:

$$\hat{x} = \arg \min_{x \in \mathbb{Z}^n} \|B^\dagger(s - Ax)\|^2. \quad (9)$$

Define $y = H' s \in \mathbb{R}^m$, $H = AB^\dagger \in \mathbb{R}^{m \times n}$, then (9) represents a closest vector problem (CVP) of lattice $L(H)$:

$$\hat{x} = \arg \min_{x \in \mathbb{Z}^n} \|y - Hx\|^2. \quad (10)$$

This CVP is different from the CVP in MIMO detection (34) because the distance distribution from $y$ to lattice $L(H)$ is not known, the lattice basis is generally not admitting Gaussian distributions, and the optimization domain of $x$ is in $\mathbb{Z}^n$ rather than a finite constellation.

III. THE HYBRID SCHEME

Our hybrid scheme to solve the CVP in (10) is described as follows. The rationale is demonstrated in Fig. 1.

Fig. 1. Exploring the vicinity of a good candidate $x^{zf} \in \mathbb{R}^3$, whose ZF parallelepiped $P(H)$ is the cyan cube. After updating the target vector $y \leftarrow y - Hx^{zf}$, to optimize $\min_{x \in \{-1, 0, 1\}^3} \|y - Hx\|$ enables locating all the blue lattice points inside the white cubes (some cubes are not plotted to avoid shading).

1) Apply lattice reduction to a not necessarily good input basis of $L(H)$ to get $H \leftarrow HU$, $U \in \text{GL}_n(\mathbb{Z})$, and use this new basis to obtain a sub-optimal candidate $\hat{x}$, e.g., $\hat{x} = x^{zf} = [H^\dagger y]$.

2) Let $y \leftarrow y - H\hat{x}$ and define a finite constraint $B^n$.

3) Use our AMP algorithm to solve:

$$x^{amp} = \arg \min_{x \in B^n} \|y - Hx\|^2. \quad (11)$$

4) Return $\hat{x} \leftarrow \hat{x} + x^{amp}$.

In order to show the hybrid scheme is valid, we try to answer the following three questions in this paper:

- To make the reduced basis good for AMP, which lattice reduction algorithm should we adopt? Answer: We should use b-LLL/b-KZ. These algorithms excel in the “short and orthogonal” metrics. See Appx. A for more details.
- Is there any theoretical/practical guarantee for transforming $x \in \mathbb{Z}^n$ to $x \in B^n$? Answer: See Secs. III-A and III-B.
- The AMP algorithms in (22), (23), (24) were assuming at least the entries of $H$ being sub-Gaussian with variance $O(1/n)$. Can we tune an AMP algorithm that is suitable for problem (11), and possibly the routines are simple and have closed-form expressions? Answer: See Sec. IV.
A. The bound of $B^n$

In the application to precoding, we show in this section that the estimation range $B^n$ is bounded after LRA precoding. We first analyze the energy efficiency $\eta_n$ of b-LLL/b-KZ aided ZF/SIC, and then address the bound for $B^n$ based on $\eta_n$.

**Definition 5.** The energy efficiency of an algorithm providing $\hat{x}$ is the smallest $\eta_n$ in the constraint
\[
\|y - H\hat{x}\| \leq \eta_n \|y - Hx^{cvp}\|,
\]
where $x^{cvp} = \arg\min_{x \in \mathbb{Z}^n} \|y - Hx\|$, and we say this algorithm solves $\eta_n$-CVP.

The practical implication of $\eta_n$ is to describe how far a suboptimal perturbation is from an optimal one.

**Theorem 1.** For the serial SIC algorithm $\epsilon$ if the lattice basis is reduced by b-LLL, then
\[
\eta_n = \beta^n / \sqrt{\beta^2 - 1},
\]
where $\beta \in (2/\sqrt{3}, \infty)$; and if the basis is reduced by b-KZ, then
\[
\eta_n = 1 + \frac{8n}{9}(n - 1)^{1+\ln(n-1)/2}.
\]

**Proof:** Regarding the b-LLL/b-KZ, their lower bounds of $r_{1,n}^2, \ldots, r_{n,n}^2$ are not worse than those of LLL/KZ, we can use the $\eta_n$ of classic LLL/KZ if they exist. So Eq. (13) is adapted from LLL in [10, Lem. 1]. Since no result about the $\eta_n$ of KZ is known, we prove a sharp bound for b-KZ in Appx. [B] where the skill involved is essentially due to [35].

**Theorem 2.** For the parallel ZF algorithm, if the lattice basis is reduced by b-LLL, then
\[
\eta_n = 2n \prod_{j=1}^n \beta^{j-1} + 1;
\]
and if the basis is reduced by b-KZ, then
\[
\eta_n = 2n \prod_{j=1}^n j^{2+\ln(j)/2} + 1.
\]

**Proof:** see Appx. [C]

**Remark 1.** Unfortunately, (15) is no better than that of LLL in [10] Lem. 1. The hardness in the analysis is to incorporate the effect of length reduction of b-LLL/b-KZ, while Thm. [2] only employs their projection conditions or diagonal reduction conditions. Since our empirical survey strongly suggests using b-LLL/b-KZ for the ZF estimator (see e.g., Figs. 6 and 9), we need Thm. [2] to claim their bounds on $\eta_n$.

$\eta_n$ is related to $B^n$ in the following way. $B$ denotes the symbol bound of $\hat{x} - x^{cvp}$. For a reduced basis, we have the following relations: $\forall i, \|H_i\| \leq \omega_i \lambda_i(H)$, $r_{i,i} \geq \lambda_i(H) / \omega_i$, and the values of $\omega_i$ and $\omega_i$ can be found in [21].

\[1\] In [10], $\eta$ is referred to as proximity factor in the CVP context. To avoid confusion with the proximity factor in [34], we simply call it “energy efficiency”.

\[2\] The readers may consult [34] if not familiar with SIC routines.

$\|y - Hx^{cvp}\|$ is bounded by the covering radius $\rho(H)$ of $\mathcal{L}(H)$, so that from the triangle inequality,
\[
\|H(x - x^{cvp})\| \leq \|y - H\hat{x}\| + \|y - Hx^{cvp}\| \\
\leq (\eta_n + 1) \rho(H).
\]

With unitary transform, we have $\|H(x - x^{cvp})\| = \|R(x - x^{cvp})\|$. Then it is reminiscent of evaluating an equality from sphere decoding:
\[
\|R(x - x^{cvp})\| \leq (\eta_n + 1) \rho(H).
\]

In the $n$th layer, one has
\[
|\hat{x}_n - x_n^{cvp}| \leq (\eta_n + 1) \rho(H)/r_{n,n} \\
\leq (\eta_n + 1) \rho(H) \omega_n / \lambda_1(H).
\]

Similarly in the $(n-1)$th layer,
\[
|\hat{x}_{n-1} - x_{n-1}^{cvp}| \leq \|R_{i,n-1} (\hat{x}_{1:n-1} - x_{1:n-1}^{cvp})/r_{n-1,n-1} \| \\
\leq (\eta_n + 1) (\rho(H) + \omega_i \lambda_i(H)) |\hat{x}_n - x_n^{cvp}| / \lambda_1(H) \\
\leq (\eta_n + 1) \rho(H) / \omega_n / \lambda_1(H) \\
+ \omega_n (\eta_n + 1) \omega_n / \lambda_1(H) \rho(H) / \lambda_1^2(H).
\]

By induction, we can obtain the upper bounds of $|\hat{x}_{n-2} - x_{n-2}^{cvp}|, \ldots, |\hat{x}_1 - x_1^{cvp}|$. The concrete values of these bounds are easily evaluated by plugging in the values of $\eta_n$, $\omega_i$ and $\omega_i$ based on the chosen LR aided ZF/SIC algorithms.

The theoretical bound of $B^n$ represents a worst case scenario. Although we have proved the existence of these upper bounds, it is not necessary to evaluate these values because, in practice, LR aided ZF/SIC are quite close to the optimal one.

B. Empirical $B^n$

In Fig. 2 we plot the maximal error $\max_i |x_i^{zf} - x_i^{cvp}|$ for the ZF estimator under $10^4$ Monte Carlo runs. Four groups of simulations are tested with system size $m = n = 8$ or $m = n = 12$, and the size of constellations set as $A = 8$ or $A = 32$. Among the four histograms inside Fig. 2 we can see that $\max_i |x_i^{zf} - x_i^{cvp}| = 1$ is the worst case behavior, and the probability of correct decoding decreases from around 30% to 10% when the system size $n$ increases from 8 to 12.

With similar settings, we have also plotted histograms of the SIC estimator. The probability of correct decoding with $n = 8$ is about 60%, and it slightly decreases to 50% when $n = 12$. The maximal symbol errors are most likely to occur with $\max_i |x_i^{sic} - x_i^{cvp}| = 1$, and there exists a small probability that $\max_i |x_i^{sic} - x_i^{cvp}| = 2$ when $n = 12$. The changes of constellation size $A$ has almost no impact on these histograms.

C. Things are ready for AMP?

Regarding the constellation of $x$, the previous discussions have demonstrated that the error of ZF/SIC estimator is bounded to a function about system dimension $n$ and some inherent lattice metrics. This means we are not facing an infinite lattice decoding problem with $Z$ constellations in Eq. (11), whence the application of AMP becomes possible.
As for the distribution of noise $w_{\text{amp}} = y - Hx$, it is not known a priori. We can equip $w_{\text{amp}}$ with a Gaussian distribution whose radius is in the order $O(\lambda_1(H))$. To be concise, let $p(w_{\text{amp}}) \sim N(0, \sigma^2 I_n)$, $\sigma^2 = O(\lambda_1(H))$. This is crucial for obtaining a non-informative likelihood function of $x$, i.e., $p(x) \sim N(H^{-1}y, \sigma^2 (H^\top H)^{-1})$.

IV. AMP ALGORITHM FOR Eq. (11)

By combining the non-informative likelihood function with the signal prior $p_X(x_i)$, we obtain a Maximum-a-Posteriori (MAP) function for Bayesian estimation:

$$p(x | y, H) \propto \prod_{a \in [m]} p_a(x, y_a) \prod_{i \in [n]} p_X(x_i),$$

(17)

where $p_a(x, y_a) = \exp(-\frac{1}{2\sigma^2}(y_a - H_{a:i}x)^2)$, and the prior $p_X(x_i)$ to be designed in subsection IV-E. The MAP function $p(x | y, H)$ is not discrete, so the measure events are extended from a power set (e.g., message passing decoding of LDPC) to a field $\mathbb{R}^n$ in the Lebesgue measure space.

The simplified belief propagation (BP) in [4] in IV-A is folklore and can be found in some pioneering literature [22], [23], [24], [51]; they are however included to help understanding the derivation in the followed subsections. After deriving our AMP algorithm, we will present the threshold functions of certain priors and characterize the symbol-wise estimation errors in Thm. [5]

A. Simplified BP

In the BP algorithm, there are $m$ factor nodes and $n$ variable nodes, indexed by $\{a, b\}$ and $\{i, j\}$ respectively. The message from variable $i$ to factor $a$ is given by

$$m_{i \to a}^{t+1}(x_i) = p_X(x_i) \prod_{b \in [m] \setminus a} m_{b \to i}^t(x_i),$$

(18)

where the message from $a$ to $i$ is

$$m_{a \to i}^t(x_i) = \int_{x \setminus x_i} \{p_a(x, y_a) \prod_{j \in [n] \setminus i} m_{j \to a}^t(x_j)\} dx.$$ 

(19)

These messages are impractical to evaluate in the Lebesgue measure space, and thus often simplified by many techniques. We attempt to remove the complexities from an expectation propagation [39] perspective. Suppose the message in Eq. (19) is estimated by a Gaussian function with mean $\alpha_{a \to i}^t / \beta_{a \to i}$

and variance $1 / \beta_{a \to i}$, then

$$m_{a \to i}^t(x_i) = N(H_{a:i}x_i; \alpha_{a \to i}^t / \beta_{a \to i}, 1 / \beta_{a \to i}).$$

By substituting Eq. (20) into Eq. (18), we have

$$m_{i \to a}^{t+1}(x_i) \propto p_X(x_i) \exp(\sum_{b \in [m] \setminus a} H_{b:i} \alpha_{b \to i}^t x_i - 1/2(\sum_{b \in [m] \setminus a} H_{b:i}^2 \beta_{b \to i} x_i + O(nH_{a:i}^3x_i^2))$$

$$\times p_X(x_i)N(x_i; u_{i \to a}, v_{i \to a}),$$

(21)

where

$$u_{i \to a}^t = \sum_{b \in [m] \setminus a} \frac{H_{b:i} \alpha_{b \to i}^t}{\sum_{b \in [m] \setminus a} H_{b:i}^2 \beta_{b \to i}},$$

(22)
\[ v_{i \rightarrow a}^t = \frac{1}{\sum_{b \in \{m \setminus a\}} H^2_{ba} \beta_{b \rightarrow i}}. \]  
\hspace{1cm} (23)

In the other direction, we work out messages \( m_{i \rightarrow a}^{t+1}(x_i) \) with Gaussian functions through matching their first and second order moments by the following constraints:

\[ m_{i \rightarrow a}^{t+1}(x_i) = \mathcal{N}(x_i; \eta(u_{i \rightarrow a}, v_{i \rightarrow a}^t), \kappa(u_{i \rightarrow a}, v_{i \rightarrow a}^t)), \]  
\hspace{1cm} (24)

\[ \eta(u_{i \rightarrow a}, v_{i \rightarrow a}^t) = \int x p_{X}(x) \mathcal{N}(x; u_{i \rightarrow a}, v_{i \rightarrow a}^t) dx, \]  
\hspace{1cm} (25)

\[ \kappa(u_{i \rightarrow a}, v_{i \rightarrow a}^t) = \int x^2 p_{X}(x) \mathcal{N}(x; u_{i \rightarrow a}, v_{i \rightarrow a}^t) dx - \eta^2(u_{i \rightarrow a}, v_{i \rightarrow a}^t), \]  
\hspace{1cm} (26)

where \( \eta(u_{i \rightarrow a}, v_{i \rightarrow a}^t) \) and \( \kappa(u_{i \rightarrow a}, v_{i \rightarrow a}^t) \) are referred to as threshold functions. From Eq. (24), inferring \( x_{i \rightarrow a}^{t+1} \) and its variance \( \varsigma_{i \rightarrow a}^{t+1} \) from \( m_{i \rightarrow a}^{t+1}(x_i) \) by using the MAP principle yields:

\[ x_{i \rightarrow a}^{t+1} = \eta(u_{i \rightarrow a}, v_{i \rightarrow a}^t), \]  
\hspace{1cm} (27)

\[ \varsigma_{i \rightarrow a}^{t+1} = \kappa(u_{i \rightarrow a}, v_{i \rightarrow a}^t). \]  
\hspace{1cm} (28)

By plugging the approximating Eq. (24) into Eq. (19), which becomes an multidimensional Gaussian function expectation \( \mathbb{E}(p_{X}(x, y_a)) \) about probability measure \( \prod_{j \in [n] \setminus a} m_{j \rightarrow a}(x_j) \), the integration over Gaussian functions becomes \( m_{i \rightarrow a}(x_i) \) as

\[ N(H_{ai}x_i; y_a - \sum_{j \in [n] \setminus i} H_{aj}x_{j \rightarrow a}^{t-1}, \sigma^2 + \sum_{j \in [n] \setminus i} |H_{aj}|^2 \varsigma_{j \rightarrow a}^{t-1}). \]  
\hspace{1cm} (29)

Comparing Eq. (29) with the previously defined mean \( \alpha_{a \rightarrow i}^t/\beta_{a \rightarrow i}^t \) and variance \( 1/\beta_{a \rightarrow i}^t \), we have

\[ \alpha_{a \rightarrow i}^t = (y_a - \sum_{j \in [n] \setminus i} H_{aj}x_{j \rightarrow a}^{t-1})/(\sigma^2 + \sum_{j \in [n] \setminus i} |H_{aj}|^2 \varsigma_{j \rightarrow a}^{t-1}), \]  
\hspace{1cm} (30)

\[ \beta_{a \rightarrow i}^t = 1/(\sigma^2 + \sum_{j \in [n] \setminus i} |H_{aj}|^2 \varsigma_{j \rightarrow a}^{t-1}). \]  
\hspace{1cm} (31)

Thus far, Eqs. (22) (23) (27) (28) (30) (31) define a simplified version of BP, where the tracking of 2mn functions in Eqs. (18) and (19) has been replaced by the tracking of 6mn scalars.

**Remark 2.** Our derivation is to equip \( m_{a \rightarrow i}(x_i) \) with a density function that can be fully described by its first and second moments, then one obtains their moment equations when passing \( m_{i \rightarrow a}(x_i) \) back. In [31] Lem. 5.3.1, Maleki had applied the Berry–Essen theorem to prove that approximating \( m_{i \rightarrow a}(x_i) \) with a Gaussian is tight. Although our variance \( 1/\beta_{a \rightarrow i}^t \) of \( m_{i \rightarrow a}(x_i) \) looks different from his, they are indeed equivalent if we set the variance \( \varsigma_{i \rightarrow a}^t \) of \( m_{i \rightarrow a}(x_i) \) as \( \sigma^2 \varsigma_{i \rightarrow a}^t \). Moreover, [31] Lem. 5.5.4 also justifies the correctness on the other side of our approximation.

### B. Reaching \( O(m + n) \) scalars

For a reduced lattice basis \( \mathbf{H} \), we denote \( \| \mathbf{h}_1 \|^2 = \sigma_1^2, \ldots, \| \mathbf{h}_n \|^2 = \sigma_n^2 \). Then the variance of entries in \( \mathbf{H} \) can be equipped, e.g., \( \forall (H_{ba}) = \sigma_b^2/m \), so one can employ this knowledge to further simplify the algorithm in [IV-A]. Here we define

\[ r_{a \rightarrow i}^t = \alpha_{a \rightarrow i}^t/\beta_{a \rightarrow i}^t = y_a - \sum_{j \in [n] \setminus i} H_{aj}x_{j \rightarrow a}^{t-1}. \]  
\hspace{1cm} (32)

By equipping all the \( \beta_{b \rightarrow i}^t \) with equal magnitude \( \forall b \), referred to as \( \bar{\beta}_{b \rightarrow i}^t \), as well as using \( \sum_{b \in \{m \setminus a\}} H^2_{ba} \approx \sigma_b^2 \) due to the law of large numbers, it yields

\[ x_{i \rightarrow a}^t = \eta\left(\frac{1}{\sigma_i^t} \sum_{b \in \{m \setminus a\}} H_{bi} r_{b \rightarrow i}^t, \frac{1}{\sigma_i^t} \bar{\beta}_{b \rightarrow i}^t\right), \]  
\hspace{1cm} (33)

\[ \varsigma_{i \rightarrow a}^t = \kappa\left(\frac{1}{\sigma_i^t} \sum_{b \in \{m \setminus a\}} H_{bi} r_{b \rightarrow i}^t, \frac{1}{\sigma_i^t} \bar{\beta}_{b \rightarrow i}^t\right). \]  
\hspace{1cm} (34)

For the moment, we can expand the local estimations about \( r_{a \rightarrow i}^t \), and \( x_{i \rightarrow a}^t \) as \( r_{a \rightarrow i}^t = r_a^t + \delta r_{a \rightarrow i}^t \), \( x_{i \rightarrow a}^t = x_i^t + \delta x_{i \rightarrow a}^t \), so the techniques in [24, 23] can be employed. The crux of these transformations is to neglect elements whose amplitudes are no larger than \( O(1/n) \). Subsequently, Eq. (32) and (33) become

\[ r_a^t + \delta r_{a \rightarrow i}^t = y_a - \sum_{j \in [n]} H_{aj} (x_{j \rightarrow a}^{t-1} + \delta x_{j \rightarrow a}^{t-1}) + H_{ai} x_{i \rightarrow a}^{t-1}, \]  
\hspace{1cm} (35)

\[ x_i^t + \delta x_{i \rightarrow a}^t = \eta\left(\frac{1}{\sigma_i^t} \sum_{b \in \{m \setminus a\}} H_{bi} (r_b^t + \delta r_{b \rightarrow i}^t), \frac{1}{\sigma_i^t} \beta_{b \rightarrow i}^t, \frac{1}{\sigma_i^t} \bar{\beta}_{b \rightarrow i}^t\right) + \frac{1}{\sigma_i^t} H_{ai} r_{a \rightarrow i}^t. \]  
\hspace{1cm} (36)

In (35), terms with \( \{i\} \) indexes are mutually related while others are not, so that

\[ r_a^t = y_a - \sum_{j \in [n]} H_{aj} (r_{j \rightarrow a}^{t-1} + \delta x_{j \rightarrow a}^{t-1}), \]  
\hspace{1cm} (37)

\[ \delta r_{a \rightarrow i}^t = H_{ai} x_{i \rightarrow a}^{t-1}. \]  
\hspace{1cm} (38)

Further expand the r.h.s. of (36) with the first order Taylor expression of \( \eta(u, v) \) at \( u_a \), in which

\[ \frac{\partial \eta(u, v)}{\partial u}
\bigg|_{u_a} = \frac{1}{\sigma_i^t} \sum_{b \in \{m \setminus a\}} H_{bi} r_{b \rightarrow i}^t, v = \frac{1}{\sigma_i^t} \bar{\beta}_{b \rightarrow i}^t = \frac{\sigma_i^t \beta_{b \rightarrow i}^t}{\sigma_i^t}, \]  
\hspace{1cm} (39)

then it yields

\[ x_i^t = \eta\left(\frac{1}{\sigma_i^t} \sum_{b \in \{m \setminus a\}} H_{bi} (r_b^t + \delta r_{b \rightarrow i}^t), \frac{1}{\sigma_i^t} \beta_{b \rightarrow i}^t, \frac{1}{\sigma_i^t} \bar{\beta}_{b \rightarrow i}^t\right) + \delta x_{i \rightarrow a}^t. \]  
\hspace{1cm} (40)
Algorithm 1: The AMP algorithm.

Input: Lattice basis $H$, target $y$, number of iterations $T$, threshold functions $\eta$ and $\kappa$, the minimum symbol error $\sigma^2$.

Output: estimated coefficient $x$.

1. $x^0 = 0$, $r^0 = y$, $\tau_0 = 10^4$;
2. $\Theta = \text{diag}(1/\text{diag}(H^\top H))$;
3. for $t = 1, \ldots, T$ do
   4. $x^t = \eta(\Theta H^\top r^t + x^{t-1}, \Theta r^2_t 1)$;
   5. $\bar{\tau}^2_t = (\Theta^{-1} \kappa(\Theta H^\top r^t + x^{t-1}, \Theta r^2_t 1))$;
   6. $r^{t+1} = y - Hx^t + \frac{n}{m} \bar{\tau}^2_t r^t$;
   7. $\tau^2_{t+1} = \sigma^2 + \frac{n}{m} x^2_t$.

C. Further simplification

From (42), the estimated variance for each $x^t_i$ now becomes

$$\varsigma^2_i = \kappa(1/\sigma^2_t \sum_{b \in [m]} H_{bi} r^t_b + x^{t-1}_i, \tau^2_i/\sigma^2_t),$$

As $\varsigma^2_i \approx \varsigma^2_{i \to b}$, $\forall b$, (31) tells

$$\beta^2_{t \to b} = 1/(\sigma^2 + \sum_{j \in [n]} \sigma^2_{j, ij} r^{t-1}_j).$$

According to (46), we denote $\beta^2_{t \to b}$ as $1/\tau^2_t$, then the whole algorithm can be described by the following four steps:

1. $x^t_i = \eta(1/\sigma^2_t \sum_{b \in [m]} H_{bi} r^t_b + x^{t-1}_i, \tau^2_i/\sigma^2_t)$;
2. $\varsigma^2_i = \kappa(1/\sigma^2_t \sum_{b \in [m]} H_{bi} r^t_b + x^{t-1}_i, \tau^2_i/\sigma^2_t)$;
3. $r^{t+1}_a = y_a - \sum_{j \in [n]} H_{aj} x^t_j + \sum_{j \in [n]} \sigma^2_{j, ij} \varsigma^2_i r^t_j / m r^2_t$;
4. $\bar{\tau}^2_t = 1/n \sum_{j \in [n]} \sigma^2_{j, ij} \varsigma^2_i$.

E. Associating discrete priors

Algo. 1 needs to work with specifically designed threshold functions. From Secs. IV-A and IV-B a dominant portion of “errors” would be corrected if we impose a ternary prior $\{-1, 0, 1\}$ for $p_X(x)$. We present its threshold functions $\eta_e(u, v)$ and $\kappa_e(u, v)$ in Lem. 1 which can be proved after a simple algebra exercise. These threshold functions have closed forms and are easy to compute. The AMP algorithm using (51) (52) due to ternary priors is referred to as APMP.

**Lemma 1.** Let $Y = X + W$, with $X \sim p_X(x) = (1 - \varepsilon) \delta(x) + \varepsilon/\delta(x - 1) + \varepsilon/\delta(x + 1), W \sim N(0, v)$. Then the conditional mean and conditional variance of $X$ on $Y$ are:

$$\eta_e(u, v) \triangleq \mathbb{E}(X|Y = u) = \frac{\sinh(u/v)}{(1 - \varepsilon)/\cosh(1/(2v)) + \cosh(u/v)},$$

$$\kappa_e(u, v) \triangleq \mathbb{V}(X|Y = u) = \frac{(1 - \varepsilon)/\cosh(u/v) + 1}{((1 - \varepsilon)/\cosh(1/(2v)) + \cosh(u/v))^2}.$$

D. Discussions

After lattice reduction and transforming the $\mathbb{Z}$ constraint to a finite set, we recognize that the AMP/GAMP algorithms in (26), (22), (29) can be employed for our problem after further regularizing the channels (i.e., let $H \leftarrow H\Theta^{1/2}$ and update the prior $x \leftarrow \Theta^{-1/2} x$). However, Algo. 1 still gives valuable insights in the following aspects:

i) We can explicitly study the impact of channel power $\{\sigma^2_1, \ldots, \sigma^2_n\}$ on the state evolution equation based on our derivation, as shown in Sec. IV-F. Moreover, $\bar{\tau}^2_{t+1}$ in Algo. 1 reveals the averaged estimation variance of $x$ and its convergence behavior, which is computationally advantageous if one needs to observe the convergence behavior and choose a candidate in the set $\{x^0, x^1, \ldots, x^T\}$ that has the best fitness value (in that the last $x^T$ corresponding to a stable fixed point may not have the best fitness). ii) The estimated $x^t$ in Algo. 1 is reflecting the MAP estimation, while AMP with $x \leftarrow \Theta^{-1/2} x$ needs additional steps to scale $x^t$ back. Regularizing AMP with $x \leftarrow \Theta^{-1/2} x$ can be detrimental in a finite accuracy processor. For instance, in the single precision floating-point arithmetic defined in IEEE-754 standard, if $u$ in $\eta(u, v)$ is operating is a scaled range where e.g. only 4 bits of mantissa are effective, then the other 20 bits in the mantissa are wasted.
F. The impact of channel power and sparsity

We first present a theorem about the state evolution equation of our model, whose proof is given in Appx. 1.

**Theorem 3.** Assume the reduced lattice basis can be modeled as \( H_{0i} \approx N(0, \sigma_i^2/m) \), and \( x_0 = x^{\text{adv}} - \hat{x} \). Let \( \hat{x} \) denote the estimation inside Algo. 4.

Then, almost surely

\[
\lim_{\tau_i \to \infty} \left\{ \left\| x_i - x_{0,i} \right\|^2, \forall i \right\} = \left\{ \mathbb{E} \left[ \sigma_i^2 \left| (X + \tau_i Z, \tau_i^2) - X^2, \forall i \right. \right\},
\]

in which \( \tau_i \), meets the following relation:

\[
\tau_i^2 = \frac{1}{\sigma_i^2} \sum_{j \in [n]} \sigma_j^2 \mathbb{E} \left[ \sigma_j^2 \left| (X + \tau_{i-1} Z, \tau_{i-1}^2) - X^2 \right. \right. + \frac{\sigma_j^2}{\tau_i^2},
\]

where the expected value is taken over two independent random variables \( Z \sim N(0, 1) \) and \( X \sim p_X \).

We call (53) a state evolution equation. Notice that if we define \( \tau_i^2 \triangleq \tau_i \sigma_j^2 \), then Eq. (53) becomes

\[
\tau_i^2 = \frac{1}{m} \sum_{j \in [n]} \sigma_j^2 \mathbb{E} \left[ \sigma_j^2 \left| (X + \tau_{i-1} \sigma_j Z, \tau_{i-1}^2 / \sigma_j^2) - X^2 \right. \right. + \sigma_j^2, \sigma_j^2,
\]

and this relation is reflected by step 7 in Algo. 4.

Based on Eq. (54), we can use Lem. 4 with \( W \sim N(0, \tau_i^2 / \sigma_j^2) \) and the expression of \( p_X(x) \) to obtain

\[
\tau_i^2 = \frac{1}{m} \sum_{j \in [n]} \sigma_j^2 \mathbb{E} \left[ (1 - \varepsilon) g_1(Z, \tau_i^2) + \varepsilon g_2(Z, \tau_i^2) \right] + \sigma_j^2,
\]

where

\[
g_1(Z, \tau_i^2) = \frac{(1 - \varepsilon) \varepsilon e^{\sigma_j^2/(2\tau_i^2)} \cos(h(Z \sigma_j / \tau_{i-1}) + 1)}{(1 - \varepsilon) \varepsilon e^{\sigma_j^2/(2\tau_i^2)} + \cosh(Z \sigma_j / \tau_{i-1})^2)},
\]

\[
g_2(Z, \tau_i^2) = \frac{(1 - \varepsilon) \varepsilon e^{\sigma_j^2/(2\tau_i^2)} \cos(h(Z \sigma_j / \tau_{i-1} + \sigma_j^2 / \tau_i^2) + 1)}{(1 - \varepsilon) \varepsilon e^{\sigma_j^2/(2\tau_i^2)} + \cosh(Z \sigma_j / \tau_{i-1} + \sigma_j^2 / \tau_i^2))^2}.
\]

\[\text{Note that this step is using an unconditional variance rather than the conditional variance in Eq. (2).}\]

In the AMP algorithm for ternary alphabets, we shall demonstrate the impact of channel power \( \{\sigma_j^2\} \) and sparsity \((1 - \varepsilon)\). The technique involved is about analyzing fixed points \([40]\). We define a function based on (55):

\[
\Psi(\tau^2) = \frac{1}{m} \sum_{j \in [n]} \sigma_j^2 \mathbb{E} \left[ (1 - \varepsilon) g_1(Z, \tau^2) + \varepsilon g_2(Z, \tau^2) \right] + \sigma_j^2.
\]

**Definition (40).** \( \tau^2 \) is called a fixed point of \( \Psi(\tau^2) \) if \( \Psi(\tau^2) = \tau^2 \), and this point is called stable if there exists \( \varepsilon \to 0^+ \), such that \( \Psi(\tau^2 + \varepsilon) < \tau^2 \) and \( \Psi(\tau^2 - \varepsilon) > \tau^2 \). When \( \Psi(0) = 0 \), the stability condition is relaxed to \( \Psi(\tau^2 + \varepsilon) < \tau^2 \). A fixed point is called unstable if it fails the stability condition.

**Proposition 1.** There exists a minimum \( \varepsilon' > 0 \), such that \( \forall \sigma_j^2 > \varepsilon' \), the highest stable fixed point of Eq. (56) is \( \Psi(\varepsilon'/m \sum_{j \in [n]} \sigma_j^2 + \sigma_j^2) = \varepsilon/m \sum_{j \in [n]} \sigma_j^2 + \sigma_j^2 \).

**Proof:** Since we have

\[
\lim_{\tau^2 \to \infty} \Psi(\tau^2) = \frac{1}{m} \sum_{j \in [n]} \sigma_j^2 \frac{(1 - \varepsilon) \varepsilon \sigma_j^2 / \tau_i^2 + \varepsilon}{(1 - \varepsilon) \varepsilon \sigma_j^2 / \tau_i^2 + \varepsilon + (1 - \varepsilon) \varepsilon + (1 - \varepsilon) / \varepsilon + 1) + \sigma_j^2}
\]

one can always tune \( \sigma_j^2 \) such that \( \Psi(\tau^2) \) intersects with \( f(\tau^2) = \tau^2 \) and the point of intersection becomes stable. This point is the highest one as \( \partial \Psi(\tau^2) / \partial \tau^2 = 0 \) for all \( \tau^2 > \varepsilon/m \sum_{j \in [n]} \sigma_j^2 + \sigma_j^2 \), which means \( \Psi(\tau^2) < \tau^2 \) in this region.

In the proposition, the highest fixed point is unique if \( \partial \Psi(\tau^2) / \partial \tau^2 < 1 \forall \tau^2 > 0 \), which means the increment of \( \Psi(\tau^2) \) is never larger than that of \( f(\tau^2) = \tau^2 \).

Prop. 4 reflects the worst case mean square error (MSE) performance of our algorithm. One implication of Prop. 4 is, a stronger lattice reduction method can help to make the fixed point smaller. E.g., with b-KZ, one has

\[
\sum_{j \in [n]} \frac{\sqrt{\lambda_j} + 3}{2} \lambda_j \leq \frac{1}{m} \sum_{j \in [n]} \sqrt{j + 3}
\]

for \( n \geq 2 \). Another implication is, the performance of AMP should be better if the real spark is small. There is however no genie granting which \( \varepsilon \) fits the actual prior. According to our simulations, \( \varepsilon = 0.5 \) is a good trade-off.

G. Complexity

The complexity is assessed by counting the number of floating-point operations (flops). For the threshold functions (51) (52) of AMPT, we can use \( \sinh(u) \approx u \), \( \cosh(u) \approx 1 + u^2/2u^2 \) for small \( u/v \) since \( \sinh(x) = \sum_{n=0}^{\infty} \frac{x^{2n+1}}{(2n+1)!} \cos(x) = \sum_{n=0}^{\infty} \frac{x^{2n+1}}{(2n+1)!} \). Outer bounding (51) (52) is also possible for large \( u/v \), so we can approximate (51) (52) by O(1) flops, respectively. The O(1) complexity also holds for (66) (67) of AMPG. In conclusion, the complexity of our AMP program is \( O(\text{mnT}) \). On the contrary, a full enumeration with a ternary constraint requires at least \( O(3^n) \) flops, and ZF/SIC requires \( O(3n^2) \) flops.
V. Simulations

In this section, we examine the symbol error rate (SER) performance and the complexity of our hybrid scheme, as well as the impact of lattice reduction and parameter selection. All the SER figures are generated from $2 \times 10^4$ Monte Carlo runs.

In the first example, we study the SNR versus SER performance of our AMP algorithms. The system size is set as $m = n = 8$ or $m = n = 14$. We use b-LLL of list size 1 as the reduction method. The benchmark algorithms serving the comparison purpose include sphere precoding, b-LLL-ZF and b-LLL-SIC. The sphere precoding method [2] which exactly solves CVP serves as the lower bound, while b-LLL-ZF/b-LLL-SIC shows the system performance before gluing the AMP algorithm. In the AMP algorithm, we set $\sigma^2 = 0.05$, $T = 20$. We set $\varepsilon = 0.5$ for AMP and $\sigma^2 = 0.5$ for AMPG. According to Fig. 5 with $n = 8$, most algorithms approach the sphere precoding lower bound except b-LLL-ZF, which is because the lattice reduction aided methods are all diversity achieving and their gaps to sphere precoding are modest in small system size. With $n = 14$, we can observe 1dB gain from b-LLL-ZF to b-LLL-AMPT, and 2dB gain from b-LLL-ZF to b-LLL-AMPT. As for the SIC estimators, the AMP&AMPG have about 1dB gain from the original b-LLL-SIC, and they are within 0.5dB distance from the optimal sphere precoding.

In the second example, we study the impact of lattice reduction algorithms. The AMP parameters as chosen as above. We use higher system size as $m = n = 20$ and adopt ZF so as to show more significant improvements. From Fig. 6 we can see that a stronger LR algorithm provides more obvious SER gain in the high SNR region. For instance, the b-LLL with 3/9 branches (b-LLL-3/9) has about 0.5/1dB improvement over the classic LLL reduction. Since the system size is larger than those of the first example, we can observe at least 2.5dB SER gain with our hybrid scheme. There should be a further gain by using b-KZ reduction, it is however excluded in the figure because simulating b-KZ consumes too much time.

In the third example, we examine the effect of choosing different spark $\varepsilon$ in AMPT. The benchmark algorithms are chosen as b-LLL aided ZF/SIC, and we set $\varepsilon \in \{0.1, 0.5, 0.9\}$. According to Fig. 7 with ZF initialization, the gain with $\varepsilon = 0.9$ is only about 1dB, while $\varepsilon = 0.9$ and $\varepsilon = 0.5$ have about 1.5dB and 2.5dB gains, respectively. It shows that $\varepsilon = 0.5$ is a good trade-off value. Similar observation is made with SIC initialization.

In the last example, we examine the complexity of our AMP algorithms. We use estimations in Sec. [V-C] to measure the complexity of ZF/SIC and AMP. As for the sphere precoding algorithm, it is implemented after b-LLL so as to decrease its complexity. All algorithms can take the benefits of b-LLL, and the complexity costed by lattice reduction is not counted for all of them. The actual complexity of sphere precoding depends on the inputs, so we count the number of nodes it visited, and assign $2k + 7$ flops to a visited node in layer $k$. From Fig. 8 we can see that AMP with a constant iteration number, e.g., $T = 10$ or $T = 20$, is adding little complexity budget to that of ZF/SIC. On the contrary, the exponential complexity of sphere precoding makes it at least 200 times more complicated than our ZF/SIC+AMP scheme in dimension $n = 22$. 
In this work, we have presented a hybrid precoding scheme for VP. The precoding problem in VP is about solving CVP in the geometry of numbers, and this problem is quite general because the signal space lies in integers $\mathbb{Z}$. After performing certain LR aided estimations, we demonstrated that the signal space have been significantly constrained, which paves the way for the application of the celebrated AMP algorithm in compressed sensing. By using the AMP algorithm with ternary prior or Gaussian prior, we can have threshold functions that enjoy closed form expressions. Our simulations showed that our hybrid scheme can provide a few dB’s gain in SER for VP, and the attached AMP algorithm is adding little complexity to that of ZF/SIC. As the extension of this work, one may investigate the hybrid scheme for other signal processing problems.

**APPENDIX A**

**B-LLL/B-KZ ARE GOOD FOR AMP**

Both the OD in lattice theory and coherence parameter $\mu(H)$ (without $l_2$-norm normalization) in compressed sensing can serve as the metric to evaluate the goodness of a basis, in which we found both metrics imply the boosted versions of LLL/KZ are better. More generally we can study the maximal correlation of $H$:

$$\sin \theta_{\min} \triangleq \min_i \| \pi_{H}^{1} h_i \| / \| h_i \|.$$ 

The goodness on $\sin \theta_{\min}$ implies virtues for both $\mu(H)$ and $\xi(H)$, where $\sin \arccos(\mu(H)) \geq \sin \theta_{\min}$, and

$$\xi(H) = \prod_{i=1}^{n} \left( \| h_i \| / \| \pi_{[h_1, \ldots, h_{i-1}]} h_i \| \right) \leq (\sin \theta_{\min})^{-n}.$$ 

According to the proof of Thm. 2, $\sin \theta_{\min}$ also controls the bound of $\eta_n$. In Fig. 9, we have plotted the maximal correlation $\sin \theta_{\min}$ of different LR algorithms.

**VI. CONCLUSIONS**

When proving the energy efficiency of b-KZ aided SIC/ZF, the following lemma would be needed. Remind that $H = QR$ is the QR factorization.

**Lemma 2 (21).** Suppose a basis $H$ is b-KZ reduced, then this basis conforms to

$$\lambda_1(H)^2 \leq \frac{8i}{9} (i-1)^{\ln(i-1)/2} r_{i,i},$$

$$\| h_i \|^2 \leq \left( 1 + \frac{2i}{9} (i-1)^{1+\ln(i-1)/2} \right) r_{i,i}^2$$

for $1 \leq i \leq n$, and

$$r_{k-j+1,k-j+1}^2 \leq \frac{8j}{9} (j-1)^{\ln(j-1)/2} r_{k,k}^2$$

for $2 \leq k \leq n$, $j \leq k$.

Under the unitary transform $Q^\top$, we aim to prove an equivalence of (12) as

$$\| \hat{y} - R \hat{x} \| \leq \eta_n \min_{\bar{x} \in \mathbb{Z}^n} \| \hat{y} - R \bar{x} \|,$$

with $\hat{y} = Q^\top y$. Let $x_{\text{vxp}} = R x_{\text{vxp}}$ be the closest vector to $\hat{y}$, and $x_{\text{sic}} = R x_{\text{sic}}$ be the vector founded by SIC. As the SIC parallelepiped generally matches the Voronoi region, we need to investigate the relation of $x_{\text{vxp}}$ and $x_{\text{sic}} = [\bar{y}_n/r_{n,n}]$ as in that in [35]. If $x_{\text{vxp}} = x_{\text{sic}}$ we only need to investigate $\eta_{n-1}$ in another $n-1$ dimensional CVP by setting $\tilde{y} = \hat{y} - r_n x_{\text{sic}}$. When this situation continues till the first layer, one clearly has $\eta_1 = 1$. Generally, we can assume that this mismatch first happens in the $k$th performance of different lattice reduction algorithms from dimension 14 to 20. This figure displays the advantages of boosted algorithms versus non-boosted algorithms, where the b-LLL with 1 to 9 branches (b-LLL-1/3/9) all outperform LLL/KZ, and b-KZ provides the best $\sin \theta_{\min}$ functioning.

**APPENDIX B**

**PROOF OF EQ. (14) IN THM. 1**

When proving the energy efficiency of b-KZ aided SIC/ZF, the following lemma would be needed. Remind that $H = QR$ is the QR factorization.

**Lemma 2 (21).** Suppose a basis $H$ is b-KZ reduced, then this basis conforms to

$$\lambda_1(H)^2 \leq \frac{8i}{9} (i-1)^{\ln(i-1)/2} r_{i,i},$$

$$\| h_i \|^2 \leq \left( 1 + \frac{2i}{9} (i-1)^{1+\ln(i-1)/2} \right) r_{i,i}^2$$

for $1 \leq i \leq n$, and

$$r_{k-j+1,k-j+1}^2 \leq \frac{8j}{9} (j-1)^{\ln(j-1)/2} r_{k,k}^2$$

for $2 \leq k \leq n$, $j \leq k$. 

Under the unitary transform $Q^\top$, we aim to prove an equivalence of (12) as

$$\| \hat{y} - R \hat{x} \| \leq \eta_n \min_{\bar{x} \in \mathbb{Z}^n} \| \hat{y} - R \bar{x} \|,$$
Lemma 3. \( \sin \theta \) condition is crucial as one already has

\[
\| \mathbf{y} - \mathbf{v} \| \geq r^2_{k,k} (\mathbf{y}/\mathbf{r}_{k,k} - x_{k}^{\text{ic}})^2 \geq r^2_{k,k}/4. \quad (61)
\]

According to (59) of b-KZ, we have \( r^2_{k,k} = \frac{2k}{9}(j - 1)^{1+\ln(k-1)/2} \), then the SIC solution \( R_{1:n,1:k}^{\text{ic}} \) satisfies

\[
\| \mathbf{y} - R_{1:n,1:k}^{\text{ic}} \| \leq \left( \frac{1}{4} + \frac{2k}{9} (k - 1)^{1+\ln(k-1)/2} \right) r^2_{k,k}. \quad (62)
\]

Combining (62) and (61), and choose \( n = \) the worst case, we have

\[
\| \mathbf{y} - \mathbf{v} \| \leq \left( 1 + \frac{8n}{9} (n - 1)^{1+\ln(n-1)/2} \right) \| \mathbf{y} - \mathbf{v} \|. \quad (63)
\]

**APPENDIX C**

**PROOF OF THM. 2**

The energy efficiency of b-LLL/b-KZ aided ZF precoding is non-trivial to prove because we cannot employ the size reduction conditions to claim an upper bound for \( (\mathbf{A})_i \) as that in [33] Eq. (65)], in which \( \mathbf{A} = R_{i:n,i:n} \). This condition is crucial as one already has

\[
\sin^2 \theta_i \geq \frac{1}{\| h_i \|^2 (\mathbf{A})_i \},
\]

according to [33] Appx. 1], where \( \theta_i \) is the angle between \( h_i \) and \( \text{span}(h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n) \). The following lemma proves a lower bound for \( \sin^2 \theta_i \) by only invoking the relation between \( \| h_i \|^2 \) and \( r^2_{i,i} \).

**Lemma 3.** Let \( \mathbf{H} \) be a b-KZ reduced basis, then it satisfies

\[
\sin^2 \theta_i \geq \left( \prod_{k=1}^{n} k^{2+\ln(k)/2} \right)^{-1}
\]

**Proof:** Define \( \mathbf{M} = R_{i:n,1:n}^{-1} \) along with \( \mathbf{M} = \frac{1}{r_{i,i}}, \) then

\[
\mathbf{M} = \begin{bmatrix} M_{k}^{-1} & \mathbf{R}_{i:k,1:k}^{-1} \\ 0 & \mathbf{I}_{k,k} \end{bmatrix}
\]

By using Cauchy–Schwarz inequality on \( \mathbf{M}_{1:k}^{k-1} \mathbf{R}_{i:k,1:k}^{-1} \) we also have

\[
\| \mathbf{M}_{1:k}^{k-1} \| \leq \frac{\| \mathbf{M}_{1:k}^{k-1} \|^{2} + \| \mathbf{R}_{i:k,1:k}^{-1} \|^{2}}{r_{i,i}^{2}}
\]

It is evident that \( \| \mathbf{R}_{i:k,1:k}^{-1} \| \leq \frac{\| \mathbf{h}_{k} \|}{r_{k,k}} \), so that

\[
\| \mathbf{M}_{1:k}^{k-1} \| \leq \frac{\| \mathbf{M}_{1:k}^{k-1} \|^{2}}{r_{i,i}^{2}} (1 + \frac{2k}{9} (k - 1)^{1+\ln(k-1)/2}). \quad (63)
\]

By induction, one has

\[
(\mathbf{A})^{-1}_{11} = \| \mathbf{M}_{1}^{n} \|^2 \geq \frac{\| \mathbf{h}_{i} \|^2 r_{i,i}^{2}}{\prod_{k=i+1}^{n} k^{2+\ln(k)/2}}
\]

and thus

\[
\sin^2 \theta_i \geq \frac{\| \mathbf{h}_{i} \|^2 r_{i,i}^{2}}{\prod_{k=i+1}^{n} k^{2+\ln(k)/2}} \geq \left( \prod_{k=i}^{n} k^{2+\ln(k)/2} \right)^{-1}
\]

where the second inequality is due to Lem. 2.

With the same technique as above, we can bound \( \sin^2 \theta_i \) for b-LLL.

**Lemma 4.** Let \( \mathbf{H} \) be a b-LLL reduced basis, then it satisfies

\[
\sin^2 \theta_i \geq \left( \prod_{k=1}^{n} k^{2+\ln(k)/2} \right)^{-1}
\]

We proceed to investigate inequality (60). Let \( \mathbf{v} = \mathbf{R}_{x^{\text{v}}} \) be the closest vector to \( \mathbf{y} \), and \( \mathbf{v} = \mathbf{R}_{x^{\text{v}}} \) be the vector found by ZF. Define \( \mathbf{v} = \sum_{i=1}^{n} \phi_i h_i \) with \( \phi_i \in \mathbb{Z} \). If \( \mathbf{v} = \mathbf{v} \), then the energy efficiency \( \eta_n \leq 1 \). If \( \mathbf{v} = \mathbf{v} \), then

\[
\| \mathbf{v} - \mathbf{v} \| \leq \sum_{j=1}^{n} |\phi_j h_j|.
\]

At the same time, we have

\[
\mathbf{v} - \mathbf{y} = \mathbf{v} - \mathbf{v} + \mathbf{v} - \mathbf{y} = (\phi_k + \frac{\phi^{x^{\text{v}}}}{k}) h_k + m',
\]

where \( m' \) is the span of \( h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n \). \( \mathbf{v} - \mathbf{y} \) is satisfied \( |\phi_k| \leq 1 \) for all \( i \), and \( k \neq \arg \max_i |\phi_i h_i| \). From Lem. 3, \( \| (\phi_k + \frac{\phi^{x^{\text{v}}}}{k}) h_k + m' \| \geq |\phi_k + \frac{\phi^{x^{\text{v}}}}{k}| \left( \prod_{j=k}^{n} j^{2+\ln(j)/2} \right)^{-1} \| h_k \|, \)

\[
\| \mathbf{v} - \mathbf{y} \| \geq |\phi_k| \left( \prod_{j=k}^{n} j^{2+\ln(j)/2} \right)^{-1} \| h_k \|
\]

as \( |\phi_k + \frac{\phi^{x^{\text{v}}}}{k}| \geq |\phi_k|/2 \). According to the triangle inequality, one has for b-KZ that

\[
\| \mathbf{v} - \mathbf{y} \| \leq \left\| \mathbf{v} - \mathbf{v} \right\| + \| \mathbf{v} - \mathbf{v} \|
\]

One can similarly prove for b-LLL that

\[
\| \mathbf{v} - \mathbf{v} \| \leq \left( 2n \prod_{j=1}^{n} j^{2+\ln(j)/2} + 1 \right) \| \mathbf{v} - \mathbf{y} \|
\]

**APPENDIX D**

**PROOF OF THM. 3**

**Proof:** We follow [36] Sec. 1.3 to analyze the state evolution equation (53). Let the observation equation be \( y^{t} = H^{t} x_0 + w \), where the prior of \( x_0 \) is denoted by \( p_x \), \( H_{bi} \sim N(0, \sigma^2/n) \), and \( w_t \in N(0, \sigma^2) \). Without the Onsager term, the residual equation becomes:

\[
r^{t} = y^{t} - H^{t} x^{t}.
\]
Along with with independently generated \( \{H^t\} \), the estimation equation becomes:

\[
x^{t+1} = \eta(\Theta H^T r^t + x^t, \Theta \tau_t^2 1).
\]

(65)

Then we evaluate the first input for the threshold function \( \eta \):

\[
\Theta H^T r^t + x^t = \begin{array}{l}
\Theta H^T (H'x_0 + w - H'x^t) + x^t \\
= x_0 + \frac{(\Theta H^T H - I)(x_0 - x^t)}{u v} + \Theta H^T w.
\end{array}
\]

Regarding term \( v \), it satisfies \( \mathbb{V}(v_i) = \frac{\tau^2_i}{m} \times \frac{1}{\sigma_i^2} \times m \times \sigma_0^2 \), which means \( v_i \sim N(0, \sigma_0^2/\sigma_i^2) \). As for the statistics of term \( u \), we need the following basic algebra to measure term \( \Theta H^T H^T H^T - I \):

Suppose that we have two independent Gaussian columns \( h_i, h_\varnothing \) whose entries are generated from \( N(c, \sigma_i^2/m) \) and \( N(c, \sigma_\varnothing^2/m) \) respectively. Then \( \forall t \neq j \), we have \( \mathbb{E}(h_i h_j) = mc^2 \) and \( \mathbb{V}(h_i h_j) = \sigma_i^2 \sigma_j^2/m + c^2 (\sigma_i^2 + \sigma_j^2) \). For \( i = j \), we have \( \mathbb{E}(||h_i||^2) = mc^2 + \sigma_i^2 \) and \( \mathbb{V}(||h_i||^2) = 2\sigma_i^4/m^2 + 4\sigma_i^2/\sigma_i^2/m \).

Further denote the covariance matrix of \( x_0 - x^t \) as \( \text{diag}(\hat{\tau}^2_{1,1}, \ldots, \hat{\tau}^2_{n,n}) \), where \( \hat{\tau}^2_{i,i} = \mathbb{E}[\eta(X + \tau_i, Z, \tau_i^2, i)] - X^2 \), \( X \sim p_X, Z \sim N(0,1) \). Then \( \{u_i\} \) are i.i.d. with zeros mean and variance

\[
\frac{\hat{\tau}^2_{i,i}}{m} + \frac{1}{\sigma_i^2} \sum_{j \neq i} \sigma_j^2 \hat{\tau}^2_{i,j},
\]

in which \( \frac{\hat{\tau}^2_{i,i}}{m} \ll \frac{1}{\sigma_i^4} \sum_{j \neq i} \sigma^2_j \hat{\tau}^2_{i,j} \) and thus negligible. The entry of \( \Theta H^T H^T r^t + x^t \) can be written as \( x_{0,i} + \tau_{i,i} Z \), where the variance of \( \tau_{i,i} Z = u_i + v_i \) satisfies

\[
\tau^2_{i,i} = \frac{1}{\sigma_i^2} \sum_{j \neq i} \sigma_j^2 \hat{\tau}^2_{i,j} + \frac{\sigma^2}{\sigma_i^2} = \left( \frac{1}{m \sigma_i^2} \sum_{j \neq i} \sigma_j^2 \right) \mathbb{E}[\eta(X + \tau_{j-1,i} Z, \tau^2_{j-1,i} Z, Z)^2] - X^2 + \frac{\sigma^2}{\sigma_i^2},
\]

where (a) comes from evaluating the covariance of \( x_0 - x^t \).

\section{Appendix E}

How to Associate General Discrete Gaussian Priors

Since we have only proved that \( \max_n \{ \hat{\tau}^2_i - \sigma^2_{\text{CVP}} \} \) is bounded by a function about dimension \( n \) and some lattice metrics, one may wonder whether a discrete Gaussian prior for \( p_X(x) \) brings some benefits. Indeed, the ternary prior can be treated as a special case of the general discrete Gaussian priors. A discrete Gaussian distribution on \( \mathbb{Z} \) with zero mean and width \( \sigma_\gamma \) is defined as

\[
\rho_{\sigma_\gamma}(z) = \frac{1}{2} e^{-z^2/(2\sigma_\gamma^2)},
\]

where \( S = \sum_{z=-\infty}^{\infty} e^{-z^2/(2\sigma_\gamma^2)} \). According to a tail bound on discrete Gaussian [42 Lem. 4.4], we have

\[
\Pr_{z \sim \rho_{\sigma_\gamma}(z)}(|z| > k \sigma_\gamma) \leq 2 e^{-k^2/2}
\]

for any \( k > 0 \). This implies that \( \rho_{\sigma_\gamma}(z) \) can be calculated from a finite range. E.g., we have \( \Pr_{z \sim \rho_{\sigma_\gamma}(z)}(|z| > 10 \sigma_\gamma) \leq 3.86 \times 10^{-22} \). If \( \sigma_\gamma = 0.1 \), then \( \rho_{\sigma_\gamma}(z) \) becomes equivalent to our ternary prior with \( \varepsilon \leq 0.5 \).

Assume that we have observed \( Y = u \) from model \( Y = X + W \), with \( X \sim p_X(x) = \rho_{\sigma_\gamma}(x), W \sim N(0,v) \). Then the threshold functions are given by

\[
\eta_d(u, v) = \frac{1}{S_k} \sum_{i = -k}^{k} le^{-\frac{2 \nu^2 - u^2}{2 v^2} - \frac{(u - v)^2}{2 v^2}},
\]

\[
\kappa_d(u, v) = \frac{1}{S_k} \sum_{i = -k}^{k} (l - \eta_d(u, v))^2 e^{-\frac{2 \nu^2 - u^2}{2 v^2} - \frac{(u - v)^2}{2 v^2}},
\]

where \( S_k = \sum_{i = -k}^{k} e^{-\frac{2 \nu^2 - u^2}{2 v^2} - \frac{(u - v)^2}{2 v^2}} \). We however stress that evaluating \( \eta_d(u, v) \) and \( \kappa_d(u, v) \) is generally computationally intensive, and the fixed points of their state evolution equation are unfathomable. Fortunately, the sum of a discrete Gaussian and a continuous Gaussian resembles a continuous Gaussian if the discrete Gaussian is not very bumpy [43 Lem. 9], so we can replace \( \rho_{\sigma_\gamma}(x) \) with \( N(x; 0, \sigma_\gamma^2) \) with properly chosen \( \sigma_\gamma^2 \). Let the signal prior be \( p_X(x) = N(x; 0, \sigma_\gamma^2) \), then it corresponds to another pair of threshold functions that have closed forms:

\[
\eta_g(u, v) = \frac{u \sigma_{\gamma}}{\sigma_\gamma^2 + v},
\]

\[
\kappa_g(u, v) = \frac{v \sigma_\gamma}{\sigma_\gamma^2 + v}.
\]

Based on Eq. (54), we can obtain its equivalent fixed point function:

\[
\Psi_g(\tau^2) \triangleq \sigma^2 + \frac{1}{m} \sum_{j \in \gamma} \frac{\tau^2_j \sigma_j^2}{\tau^2_j + \sigma_j^2 \sigma_\gamma^2}.
\]

(68)

\( \Psi_g(\tau^2) \) is proportional to \( \tau^2 \). Define \( \sigma_{\min}^2 \triangleq \min_j \sigma_j^2 \) and \( \sigma_{\max}^2 \triangleq \max_j \sigma_j^2 \), we also have

\[
\frac{m \tau^2_j \sigma_{\min}^2 \sigma_\gamma^2}{\tau^2_j + \sigma_{\min}^2 \sigma_\gamma^2} \leq \Psi_g(\tau^2) - \sigma^2 \leq \frac{m \tau^2_j \sigma_{\max}^2 \sigma_\gamma^2}{\tau^2_j + \sigma_{\max}^2 \sigma_\gamma^2}.
\]

As a consequence, one can easily prove that Eq. (68) has a unique stable fixed point that satisfies \( \tau^2 \in [\tau^2_{\min}, \tau^2_{\max}] \), where

\[
\tau^2_{\min} = \frac{1}{2} \left( \sigma^2 + \left( \frac{n}{m} - 1 \right) \sigma^2_{\min} \sigma_\gamma^2 \right)
\]

\[
+ \frac{1}{2} \left[ \sigma^2 + \left( \frac{n}{m} - 1 \right) \sigma^2_{\min} \sigma_\gamma^2 \right]^2 + 4 \sigma^2_{\min} \sigma_\gamma^2,
\]

and \( \tau^2_{\max} \) is defined by replacing \( \sigma^2_{\min} \) with \( \sigma^2_{\max} \) in (69). In order to make the fixed point small, one should also make the lattice basis short. The setting of \( \sigma_\gamma^2 \) is however a trade-off: it should be set smaller to yield a lower fixed point, but there should be a minimum for it so that the imposed prior still reflects discrete Gaussian information.
