Quadratically Constrained Two-way Adversarial Channels

Yihan Zhang*, Shashank Vatedka†, Sidharth Jaggi*
*Dept. of Information Engineering, The Chinese University of Hong Kong, Hong Kong SAR
†Dept. of Electrical Engineering, Indian Institute of Technology, Hyderabad, India

***Abstract*—We study achievable rates of reliable communication in a power-constrained two-way additive interference channel over the real alphabet where communication is disrupted by a power-constrained jammer. This models the wireless communication scenario where two users Alice and Bob, operating in the full duplex mode, wish to exchange messages with each other in the presence of a jammer, James. Alice and Bob simultaneously transmit their encodings $\underline{x}_A$ and $\underline{x}_B$ over n channel uses. It is assumed that James can choose his jamming signal $\underline{s}$ as a noncausal randomized function of $\underline{x}_A + \underline{x}_B$, and the codebooks used by Alice and Bob. Alice and Bob observe $\underline{x}_A + \underline{x}_B + \underline{s}$, and must recover each others' messages reliably. In this article, we provide upper and lower bounds on the capacity of this channel which match each other and equal $\frac{1}{2}\log\left(\frac{1}{2} + \mathsf{SNR}\right)$ in the high-SNR regime (where SNR, *signal to noise ratios*, is defined as the ratio of the power constraints of the users to the power constraint of the jammer). We give a code construction based on lattice codes, and derive achievable rates for large SNR. We also present upper bounds based on two specific attack strategies for James. Along the way, sumset property of lattices for the achievability and general properties of capacity-achieving codes for memoryless channels for the converse are proved, which might be of independent interest. The full version of this paper is [1].**

I. Introduction

Our work is motivated by jamming in multiuser wireless channels. Consider two users Alice and Bob who wish to exchange independent messages (assumed to be uniformly distributed in a set of size 2^{nR}) with each other over the wireless medium. The communications is disrupted by an adversarial jammer, James, who injects additive noise into the channel. We assume that all three parties operate in the full-duplex mode, which means that they are able to transmit and receive simultaneously. Alice and Bob encode their messages into n-length sequences $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}_B$ with real valued components and are simultaneously transmitted across the channel. At the same time, James transmits a jamming sequence $\underline{\mathbf{s}}$. The channel is additive, and each user gets to observe $\underline{\mathbf{y}} = \underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B + \underline{\mathbf{s}}$. The goal of the two users is to recover each others' message reliably from this observation.

The signals transmitted by Alice, Bob and James are required to satisfy quadratic power constraints of nP, nP, and nN respectively, i.e., $\|\underline{\mathbf{x}}_A\|^2 \leqslant nP$, $\|\underline{\mathbf{x}}_B\|^2 \leqslant nP$, $\|\underline{\mathbf{s}}\|^2 \leqslant nN$. We assume that James can select his jamming signal $\underline{\mathbf{s}}$ as a noncausal function of $\underline{\mathbf{z}} \coloneqq \underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B$, and also the codebooks/coding strategies used by Alice and Bob. However, James has no additional information about the messages or the transmitted signals in addition to that revealed by $\underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B$ and the users' codebooks. We call this the (P, N) quadratically constrained two-way adversarial channel problem. This is illustrated in Fig. 1.

The goal is to design sequences of encoders and decoders for Alice and Bob such that the probability of error of decoding the respective messages is vanishing in n. Here, the randomness is over the encoding processes used by Alice and Bob, as well as the jamming signal. We say that a rate R is achievable if there exist sequences of codes for which the associated probabilities of decoding error is vanishing in n, and the capacity is the supremum of all achievable rates.

In this paper, we give an upper bound on the capacity. We show that reliable communication is impossible for $N \geqslant 3P/4$. For $N < 3P/4$, we show that the capacity is upper bounded by $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)$. We also describe a coding scheme which shows that for sufficiently large values of P/N, this bound is achievable.

The problem considered in this paper falls under the general setup of arbitrarily varying channels (AVCs), introduced in [2]. This framework is a good model for channels where the noise statistics are arbitrary and unknown, and also where communication is disrupted by active adversaries. Much of the literature has focused on point-to-point communication where Alice wants to send a message to Bob, and James attempts to jam the transmission. The quadratically constrained point-to-point AVC (also called the Gaussian AVC) was studied in [3], who gave upper and lower bounds on the capacity of the channel under the assumption that James observes a noiseless version of the transmitted codeword (a.k.a. the *omniscient* adversary). Later, [4] and [5] studied the problem with an "oblivious" James, who knows the codebook, but does not see the transmitted codeword. They showed that under an average probability of error metric, the capacity of the oblivious adversarial channel is equal to $\frac{1}{2}\log\left(1 + \frac{P}{N}\right)$ when $P > N$ and zero otherwise.

Successive works have characterized the error exponent of the oblivious Gaussian AVC [6], capacity of the oblivious vector Gaussian AVC [7], and the Gaussian AVC with an unlimited amount of shared secret key between Alice and Bob [8]. Sarwate [9], and later Zhang et al. [10] studied the myopic AVC, where James can choose his jamming vector as a function of the codebooks and a noisy copy of the transmitted signal. A related model was studied by in [11], who assumed that James knows the message, but not the exact codeword

The work of Sidharth Jaggi and Yihan Zhang was supported by the Research Grants Council (RGC) of Hong Kong under Project Numbers 14300617, 14304418 and 14301519.

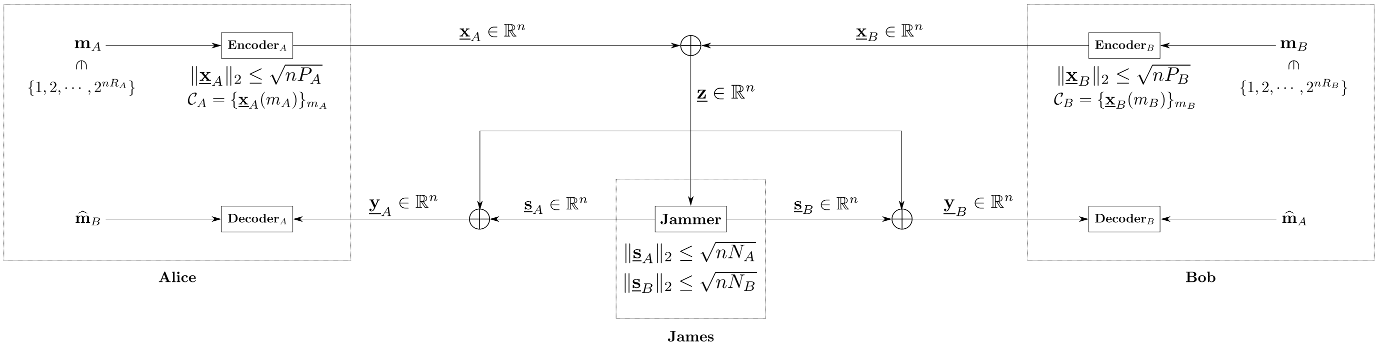
$\mathbf{m}_A$
$\{1, 2, \cdots, 2^{nR_A}\}$
Encoder$_A$
$\|\underline{\mathbf{x}}_A\|_2 \le \sqrt{nP_A}$
$\mathcal{C}_A = \{\underline{\mathbf{x}}_A(m_A)\}_{m_A}$
$\underline{\mathbf{x}}_A \in \mathbb{R}^n$
$\underline{\mathbf{x}}_B \in \mathbb{R}^n$
Encoder$_B$
$\mathbf{m}_B$
$\|\underline{\mathbf{x}}_B\|_2 \le \sqrt{nP_B}$
$\mathcal{C}_B = \{\underline{\mathbf{x}}_B(m_B)\}_{m_B}$
$\{1, 2, \cdots, 2^{nR_B}\}$
$\underline{\mathbf{z}} \in \mathbb{R}^n$
$\widehat{\mathbf{m}}_B$
Decoder$_A$
$\underline{\mathbf{y}}_A \in \mathbb{R}^n$
$\underline{\mathbf{s}}_A \in \mathbb{R}^n$
Jammer
$\underline{\mathbf{s}}_B \in \mathbb{R}^n$
$\underline{\mathbf{y}}_B \in \mathbb{R}^n$
Decoder$_B$
$\widehat{\mathbf{m}}_A$
$\|\underline{\mathbf{s}}_A\|_2 \le \sqrt{nN_A}$
$\|\underline{\mathbf{s}}_B\|_2 \le \sqrt{nN_B}$
Alice
Bob
James

Fig. 1: A quadratically constrained two-way adversarial channel.

transmitted by Alice. Game-theoretic versions of the problems have also been considered in the literature, including the point-to-point case [12], with multiple antennas at the transmitter and receiver [13], and also the two-sender scenario [14]. The list decoding capacity under the oblivious and omniscient cases were studied in [15] and [16] respectively.

Multiuser AVCs have received attention only very recently. Multiple access channels with adversarial jamming were studied in [17], [18]. The capacity of the relay channel was analyzed in [19], while [20] gave inner and outer bounds on the capacity region of the degraded broadcast channel with side information at the encoder.

The work most related to our paper is that on the discrete-alphabet two-way additive channel with an adversarial jammer which was studied in [21]. They showed that for discrete additive channels over $\mathbb{F}_q$ where James' transmissions must satisfy a Hamming weight constraint of p, the capacity is equal to $1 - H_q(p)$. In other words, James can do no worse (to Bob)[1] than transmitting random noise. Many of our ideas were inspired by this work, and we will elaborate on this in the coming sections. However, the conclusions that we can draw about the quadratically constrained case are different. In particular, the capacity is *lower* than what we would get if the noise vector were Gaussian. A game-theoretic version of the quadratically constrained case we study here was studied in [22].

II. Overview of our results

First consider symmetric case where $P_A = P_B = P$ and $N_A = N_B = N$. For a (P, N) quadratically constrained two-way adversarial channel, let $\mathsf{SNR} := P/N$ be the *signal-to-noise ratio*. Let C_A and C_B denote the capacities of Alice and Bob, respectively. All of our results hold under the worst-case jamming policy employed by James.

Theorem 1 (Achievability)**.** *For a (P, N) quadratically constrained two-way adversarial channel, there exists a function g with $g(\delta) \xrightarrow{\delta \to 0} \infty$, such that given any sufficiently small constant $\delta > 0$, if $\mathsf{SNR} > g(\delta)$, then both users can achieve rate $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right) - \delta$. That is, $C_A \geqslant \left[\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)\right]^+$ and $C_B \geqslant \left[\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)\right]^+$.*

Theorem 2 (Converse)**.** *For a (P, N) quadratically constrained two-way adversarial channel, for any sufficiently small constant $\delta > 0$, neither of the users can achieve rate larger than $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right) + \delta$. That is, $C_A \leqslant \left[\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)\right]^+$ and $C_B \leqslant \left[\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)\right]^+$.*

Corollary 3 (Capacity)**.** *For a (P, N) quadratically constrained two-way adversarial channel, there exists a function g with $g(\delta) \xrightarrow{\delta \to 0} \infty$, such that given any sufficiently small constant $\delta > 0$, if $\mathsf{SNR} > g(\delta)$, then $\lim_{\delta \to 0} C_A = \lim_{\delta \to 0} C_B = \left[\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)\right]^+$.*

Both our achievability and converse results can be trivially generalized to the asymmetric case, where the transmissions of Alice and Bob must satisfy $\|\underline{\mathbf{x}}_A\|^2 \leqslant nP_A, \|\underline{\mathbf{x}}_B\|^2 \leqslant nP_B$, James can independently jam the received vectors of Alice and Bob with jamming signals $\underline{\mathbf{s}}_A$ and $\underline{\mathbf{s}}_B$ which must satisfy $\|\underline{\mathbf{s}}_A\|^2 \leqslant nN_A, \|\underline{\mathbf{s}}_B\|^2 \leqslant nN_B$. Here Alice and Bob respectively receive $\underline{\mathbf{y}}_A = \underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B + \underline{\mathbf{s}}_A$ and $\underline{\mathbf{y}}_B = \underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B + \underline{\mathbf{s}}_B$. For this (P_A, P_B, N_A, N_B) quadratically constrained two-way adversarial channel, let $\mathsf{SNR}_A := P_B/N_A$ and $\mathsf{SNR}_B := P_A/N_B$ be the SNRs of user one and two, respectively. Then we have

Corollary 4 (Capacity, asymmetric case)**.** *For a (P_A, P_B, N_A, N_B) quadratically constrained two-way adversarial channel, there exist functions g_1, g_2 with $g_i(\delta) \xrightarrow{\delta \to 0} \infty$, $i = 1, 2$, such that given any sufficiently small constants $\delta_1, \delta_2 > 0$, if $\mathsf{SNR}_A > g_1(\delta_1)$ and $\mathsf{SNR}_B > g_2(\delta_2)$, then $C_A = \left[\frac{1}{2}\log\left(\frac{P_A}{P_A + P_B} + \frac{P_B}{N_A}\right)\right]^+$ and $C_B = \left[\frac{1}{2}\log\left(\frac{P_B}{P_A + P_B} + \frac{P_A}{N_B}\right)\right]^+$.*

Note that the capacity $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)$ vanishes when $N \geqslant 2P$ or $\mathsf{SNR} \leqslant 1/2$. Though the capacity theorem indicates that $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)$ is the capacity in high-SNR regime, we do not believe that this is tight in all regimes. Our intuition comes from the following improved converse result. We are able to push the boundary of zero-rate regime inward via certain symmetrization strategy which we call $\underline{\mathbf{z}}$*-aware symmetrization*.

Theorem 5 (Upper bounds)**.** *For a (P, N) quadratically constrained two-way adversarial channel, neither of the users can achieve positive rate if $N > 3P/4$, or $\mathsf{SNR} < 4/3$.*

Again, the above theorem can be trivially generalized to the asymmetric case which reads as follows.

[1] Said differently, transmitting random noise is James' optimal policy.

Theorem 6 (Upper bounds)**.** *For a (P_A, P_B, N_A, N_B) quadratically constrained two-way adversarial channel, user one cannot achieve positive rate if $N_A > \frac{2P_B+P_A}{4}$; user two cannot achieve positive rate if $N_B > \frac{2P_A+P_B}{4}$.*

III. Techniques, related work and proof sketch

Our ideas are inspired by [21], which characterized the capacity of the discrete additive two-way channel with a jammer. They showed that using randomly expurgated *linear* codebooks for Alice and Bob achieves the symmetric capacity $1 - H_q(p)$, where $H_q(p)$ denotes the q-ary entropy of p. This implies that James can do no worse (to Bob) than transmitting random noise. It was also observed that neither linear codes nor uniformly random codebooks can achieve the capacity of this channel. Indeed, our codebook design closely mimics [21]: we use randomly expurgated lattice codebooks.

Unlike the discrete case studied in [21], the setup we study in this paper poses additional challenges. In our setup, if the additive noise were random Gaussian with independent and identically distributed (i.i.d.) $\mathcal{N}(0, N)$ components, then the capacity is equal to $\frac{1}{2}\log_2\left(1 + \frac{P}{N}\right)$. However, we give a converse to show that the capacity is in fact strictly below this. An important observation is that the capacity of the *discrete* additive adversarial two-way channel is equal to the list decoding capacity (which also turns out to be the capacity with random noise). Unlike the discrete case, we show that the capacity of the (P, N) quadratically constrained two-way adversarial channel is (for large values of P/N) strictly above the list decoding capacity which equals $\frac{1}{2}\log\frac{P}{N}$ [23].

1) Proof techniques for upper bound: We provide three separate converse bounds for this problem by providing three attack strategies for James:

- Clearly, if $P \leqslant N$, then James can transmit a random codeword from Alice's (resp. Bob's) codebook chosen independently of everything else. Over the randomness in the choice of the codeword, Bob (resp. Alice) will then be unable to distinguish between the codewords transmitted by Alice (resp. Bob) and James. Hence, the capacity is zero.
- We can improve this to show that the capacity is zero for $N \geqslant 3P/4$. James independently selects a random codeword $\underline{\mathbf{x}}'_A$ from Alice's codebook and transmits $-\frac{1}{2}(\underline{\mathbf{z}} - \underline{\mathbf{x}}'_A)$ whenever he has enough power. With high probability (w.h.p.), this attack vector satisfies the power constraint, and Bob receives $0.5\underline{\mathbf{x}}_B + 0.5(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}'_A)$. Bob cannot decide whether $\underline{\mathbf{x}}_A$ or $\underline{\mathbf{x}}'_A$ was transmitted, and therefore the probability of error is bounded away from zero.
- In the regime when $N \leqslant 3P/4$, we define a different attack for James. He can transmit $\underline{\mathbf{s}} = -\alpha\underline{\mathbf{z}} + \underline{\mathbf{g}}$, where $\underline{\mathbf{g}} \sim \mathcal{N}(0, \gamma^2\mathbf{I}_n)$ and α, γ are constants that can be optimized over. This instantiates an effective AWGN channel for Bob (resp. Alice) which implies that the capacity cannot exceed that of this effective AWGN channel. Upon optimizing the constants, we get that the capacity cannot be any larger than $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{N}\right)$. To prove this, we analyze general properties of the empirical properties of capacity-achieving codes for the AWGN channel (which we call AWGN-good codes) which we believe are novel results and might be of independent interest. We show that independent codewords chosen uniformly from any AWGN-good code are approximately orthogonal w.h.p.

To give a flavour of our proof techniques, we briefly outline the approach used to prove the second statement.

Lemma 7. *For a (P, N) quadratically constrained two-way adversarial channel, assume $N = 3P(1+\varepsilon)/4$ for some constant $\varepsilon > 0$. Then any codebook pair $(\mathcal{C}_A, \mathcal{C}_B)$ of sizes $|\mathcal{C}_A| \geqslant \frac{\varepsilon}{2(1+\varepsilon)}$ and $|\mathcal{C}_B| \geqslant \frac{\varepsilon}{2(1+\varepsilon)}$ has average error probabilities $P_{e,avg,A} \geqslant \frac{\varepsilon}{4(1+\varepsilon)}$ and $P_{e,avg,B} \geqslant \frac{\varepsilon}{4(1+\varepsilon)}$.*

Proof. WLOG we assume that $\mathbb{E}\left[\underline{\mathbf{x}}_A\right] = \mathbb{E}\left[\underline{\mathbf{x}}_B\right] = \underline{0}$ where $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}_B$ are uniform in $\mathcal{C}_A$ and $\mathcal{C}_B$, respectively.

Define $\underline{\widetilde{\mathbf{s}}} = -\frac{1}{2}(\underline{\mathbf{z}} - \underline{\mathbf{x}}'_A) = -\frac{1}{2}(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B - \underline{\mathbf{x}}'_A)$, where $\underline{\mathbf{x}}'_A$ is a random codeword from $\mathcal{C}_A$. Define $\underline{\mathbf{s}}$ as follows.

$$\underline{\mathbf{s}} = \begin{cases} \underline{\widetilde{\mathbf{s}}}, & \|\underline{\widetilde{\mathbf{s}}}\|_2 \leqslant \sqrt{nN} \\ \sqrt{nN}\frac{\underline{\widetilde{\mathbf{s}}}}{\|\underline{\widetilde{\mathbf{s}}}\|_2}, & \text{otherwise} \end{cases}.$$

Define error events $\mathcal{E}_1 := \left\{\|\underline{\widetilde{\mathbf{s}}}\|_2 > \sqrt{nN}\right\}, \mathcal{E}_2 := \{\underline{\mathbf{x}}_A = \underline{\mathbf{x}}'_A\}$. Under the above jamming strategy, Bob receives $\underline{\mathbf{y}}_B = \frac{1}{2}(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}'_A) + \frac{1}{2}\underline{\mathbf{x}}_B$. If $\underline{\widetilde{\mathbf{s}}}$ satisfies power constraint, cancelling his own signal, Bob effectively receives $\underline{\widetilde{\mathbf{y}}}_B = \frac{1}{2}(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}'_A)$. If neither $\mathcal{E}_1$ nor $\mathcal{E}_2$ happen, then Bob has no way to distinguish between $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}'_A$ and the decoding error probability is at least $1/2$ under any decoding rule.

We now formally lower bound the probability of error under such a jamming strategy.

$$\begin{aligned} P_{\mathrm{e},B} &= \Pr\left[\widehat{\mathbf{m}}_A \neq \mathbf{m}_A\right] \\ &\geqslant \Pr\left[\{\widehat{\mathbf{m}}_A \neq \mathbf{m}_A\} \cap \mathcal{E}_1^c \cap \mathcal{E}_2^c\right] \\ &= \Pr\left[\mathcal{E}_1^c \cap \mathcal{E}_2^c\right]\Pr\left[\widehat{\mathbf{m}}_A \neq \mathbf{m}_A | \mathcal{E}_1^c \cap \mathcal{E}_2^c\right] \\ &\geqslant \frac{1}{2}(1 - \Pr\left[\mathcal{E}_1\right] - \Pr\left[\mathcal{E}_2\right]). \end{aligned}$$

First note that $\Pr\left[\mathcal{E}_2\right] = 1/|\mathcal{C}_A|$ which is at most $\frac{\varepsilon}{2(1+\varepsilon)}$ as long as $|\mathcal{C}_A| \geqslant \frac{2(1+\varepsilon)}{\varepsilon}$.

We next upper bound $\Pr\left[\mathcal{E}_1\right]$. Suppose $N = \frac{3}{4}P(1+\varepsilon)$. By Markov's inequality, $\Pr\left[\mathcal{E}_1\right] = \Pr\left[\|\underline{\widetilde{\mathbf{s}}}\|_2 > \sqrt{nN}\right] \leqslant \frac{\mathbb{E}\left[\|\underline{\widetilde{\mathbf{s}}}\|_2^2\right]}{nN}$. It suffices to upper bound $\mathbb{E}\left[\|\underline{\widetilde{\mathbf{s}}}\|_2^2\right]$.

$$\begin{aligned} &\mathbb{E}\left[\|\underline{\widetilde{\mathbf{s}}}\|_2^2\right] = \mathbb{E}\left[\left\|-\frac{1}{2}(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B - \underline{\mathbf{x}}'_A)\right\|_2^2\right] \\ =&\frac{1}{4}\Big(\mathbb{E}\left[\|\underline{\mathbf{x}}_A\|_2^2\right] + \mathbb{E}\left[\|\underline{\mathbf{x}}_B\|_2^2\right] + \mathbb{E}\left[\|\underline{\mathbf{x}}'_A\|_2^2\right] + 2\mathbb{E}\left[\langle\underline{\mathbf{x}}_A, \underline{\mathbf{x}}_B\rangle\right] \\ &\quad - 2\mathbb{E}\left[\langle\underline{\mathbf{x}}_A, \underline{\mathbf{x}}'_A\rangle\right] - 2\mathbb{E}\left[\langle\underline{\mathbf{x}}_B, \underline{\mathbf{x}}'_A\rangle\right]\Big) \\ \leqslant&\frac{1}{4}(nP + nP + nP) = 3nP/4. \end{aligned}$$

Then we get that $\Pr\left[\mathcal{E}_1\right] \leqslant \frac{3nP/4}{nN} = \frac{1}{1+\varepsilon}$. Substituting the above bound back and simplifying, we get the result. □

2) Proof techniques for lower bound: Let us briefly summarize the main elements of the achievability proof in [21]. A key step used is that even after expurgation, James is sufficiently confused about the transmitted codeword: if $\mathcal{C}_A$ and $\mathcal{C}_B$ are the codebooks obtained by independent random expurgations of the original linear code $\mathcal{C}$, then $|\mathcal{C}_A+\mathcal{C}_B| \approx |\mathcal{C}_A|$ and leaks very little information about the individual codewords to James. As a consequence, James cannot "push" the transmitted codeword to the nearest codeword in the corresponding codebook. The final step is to show that as long as the original code is list decodable with small list sizes, the expurgated code is uniquely decodable w.h.p. (over the randomness in the code expurgation).

Unlike the discrete case, we are not able to prove a matching lower bound on the capacity for all values of P, N. We show that for sufficiently large P/N, the capacity is $C = \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{N}\right)$. The code for Alice and Bob is obtained by independently expurgating a lattice code with spherical shaping (to satisfy power constraint). What makes the quadratically constrained case more challenging than the discrete one is that due to the power constraint, the sum of two codewords leaks information about the individual codewords. However, if the original lattice code is suitably chosen, then we can show that James is sufficiently confused. Even then, following the approach in [21] gets us to only the list decoding capacity of $\frac{1}{2}\log\frac{P}{N}$. To improve the rate, we introduce a proof technique inspired by [23]. We show that for every attack vector that James can instantiate, the effective decoding region is significantly smaller than $\mathcal{B}^n(\underline{\mathbf{y}}, \sqrt{nN})$[2] w.h.p. (over the randomness in the choice of message).

3) Codebook: Let Λ be a lattice obtained by lifting random linear codes $\mathcal{C}'$ over a prime field $\mathbb{F}_q$ via Construction-A[3]. Specifically, let $\mathbf{G} \sim \mathbb{F}_q^{n\times k}$ be a uniformly random matrix. The field size q and dimension k will be fixed later. Define the random linear code generated by $\mathbf{G}$ as $\mathcal{C}' = \mathbf{G}\mathbb{F}_q^k$. Define $\Lambda = \frac{1}{q}\Phi(\mathcal{C}') + \mathbb{Z}^n$, where $\Phi\colon \mathbb{F}_q \to \mathbb{Z}$ is the natural embedding which maps any field element $j \in \mathbb{F}_q$ to an integer $j \in \mathbb{Z}$. One can easily check that Λ is indeed a lattice. Fix some gap-to-capacity factor $\beta > 0$. Scale Λ so as to ensure $\left|\Lambda \cap \mathcal{B}^n\left(\underline{0}, \sqrt{nP}\right)\right| \geqslant 2^{\frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{N}\right)-h(\beta)}$, where $h(\beta) \gg \beta$ satisfies $h(\beta) \xrightarrow{\beta\to 0} 0$.[4] Our lattice code is finally defined as $\mathcal{C} := \Lambda \cap \mathcal{B}^n\left(\underline{0}, \sqrt{nP}\right)$. It was shown in [24] and [25] that for suitably chosen q and k,[5] as long as $r_{\text{eff}}(\Lambda) \geqslant \sqrt{nN}2^{\beta}$, w.h.p. over $\mathbf{G}$, Λ is good for covering and simultaneously $\left(1-\frac{N}{2P}\right)\Lambda$ is $(\widetilde{N}, L)$-list-decodable, where $L = 2^{\mathcal{O}\left(\frac{1}{\beta}\log^2\frac{1}{\beta}\right)}$. Here a (sequence of) lattice $\Lambda \leqslant \mathbb{R}^n$ is said to be *good for covering* if $r_{\text{cov}}(\Lambda)/r_{\text{eff}}(\Lambda) \xrightarrow{n\to\infty} 1$; and Λ is said to be *(N, L)-list decodable* if for every $\underline{y} \in \mathbb{R}^n$, $\left|\Lambda \cap \mathcal{B}^n\left(\underline{y}, \sqrt{nN}\right)\right| \leqslant L$.

Alice's codebook $\mathcal{C}_A$ is obtained by independently picking each vector in $\mathcal{C}$ with probability $2^{-n\gamma}$ for a sufficiently small $\gamma > 0$. With high probability over this expurgation process, the transmission rate[6] is at least $\frac{1}{2}\log\left(1+\frac{P}{N}\right) - h(\beta) - \gamma$. Bob's codebook $\mathcal{C}_B$ is obtained in a similar fashion, but the expurgation process is independent of $\mathcal{C}_A$. For the convenience of future calculations, define $r_{\text{cov}}(\Lambda) := \sqrt{n\omega}$ and $r_{\text{eff}}(\Lambda) := \sqrt{n\tau}$. We take $\tau = N2^{2\beta}$. By covering-goodness, $\omega = \tau(1+\varepsilon_n)$ for some $\varepsilon_n \xrightarrow{n\to\infty} 0$.

The encoding process is deterministic, and encoder is an arbitrary deterministic map from the set of messages to the codebook.

4) Decoding rule: Bob computes $\widehat{\alpha} := 1 - \frac{\langle \underline{\mathbf{y}}_B, \underline{\mathbf{x}}_B\rangle}{nP}$, $\underline{\widetilde{\mathbf{y}}}_B := \underline{\mathbf{y}}_B - (1-\widehat{\alpha})\underline{\mathbf{x}}_B$ and $r_{\text{dec}} := \sqrt{\left\|\underline{\mathbf{y}}_B\right\|_2^2 - 2(1-\widehat{\alpha})\left\langle \underline{\mathbf{y}}_B, \underline{\mathbf{x}}_B\right\rangle}$. If there is a single codeword $\underline{\mathbf{x}}_A \in \mathcal{C}_A \cap \frac{1}{1-\widehat{\alpha}}\mathcal{B}^n(\underline{\widetilde{\mathbf{y}}}_B, r_{\text{dec}})$, then the decoder outputs the message associated to $\underline{\mathbf{x}}_A$. Otherwise, it declares an error. Alice's decoder operates likewise.

5) Intuition: We provide intuition behind our posterior-estimation-style decoding rule. All slack factors will be omitted in the rough calculations in this section.

Before proceeding, we would like to remind the readers of a fact from high dimensional geometry: as long as the $r_{\text{cov}}(\Lambda)$ is sufficiently small, a random lattice point in a ball is concentrated near the surface of the ball and is approximately orthogonal to any given vector.

Consider transmission from Alice to Bob. James' jamming vector can be generically decomposed into directions parallel and perpendicular to $\underline{\mathbf{z}}$, $\underline{\mathbf{s}}_B = -\alpha\underline{\mathbf{z}} + \underline{\mathbf{s}}_\perp = -\alpha(\underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B) + \underline{\mathbf{s}}_\perp$, where $\underline{\mathbf{s}}_\perp = \operatorname{proj}_{\underline{\mathbf{z}}^\perp}(\underline{\mathbf{s}}_B)$ is orthogonal to $\underline{\mathbf{z}}$. He has to choose α so that $\underline{\mathbf{s}}_B$ does not violate his power constraint, $\|-\alpha\underline{\mathbf{x}}_A - \alpha\underline{\mathbf{x}}_B + \underline{\mathbf{s}}_\perp\|_2^2 \approx 2\alpha^2 nP + \|\underline{\mathbf{s}}_\perp\|_2^2 \leqslant nN$. This imposes a constrain on α: $|\alpha| \leqslant \sqrt{\frac{N}{2P}}$. Under this decomposition, Bob's received word can be written as $\underline{\mathbf{y}}_B := (1-\alpha)\underline{\mathbf{x}}_A + (1-\alpha)\underline{\mathbf{x}}_B + \underline{\mathbf{s}}_\perp$. From James' view, if $\underline{\mathbf{z}}$ is typical (i.e., $\|\underline{\mathbf{z}}\|_2 \in \sqrt{2\alpha^2 P(1\pm\delta)}$), there is a large number of pairs of codewords $(\underline{\mathbf{x}}_A, \underline{\mathbf{x}}_B)$ that were potentially transmitted (i.e., $\underline{\mathbf{x}}_A + \underline{\mathbf{x}}_B = \underline{\mathbf{z}}$). Furthermore, these codewords are uniformly distributed in a thin strip $\mathcal{T}$ near the surface of $\mathcal{B}^n\left(\underline{0}, \sqrt{nP}\right)$, orthogonal to $\underline{\mathbf{z}}$, of radius approximately $\sqrt{nP/2}$. (See Fig. 2 for the geometry.) Hence the value of $\left\langle \underline{\mathbf{y}}_B, \underline{\mathbf{x}}_B\right\rangle = \langle (1-\alpha)\underline{\mathbf{x}}_A + (1-\alpha)\underline{\mathbf{x}}_B + \underline{\mathbf{s}}_\perp, \underline{\mathbf{x}}_B\rangle$ is well concentrated around $0 + (1-\alpha)\|\underline{\mathbf{x}}_B\|_2^2 + 0 \approx (1-\alpha)nP$ w.h.p. over message selection. Thereby the value of α that was chosen by James can be well estimated by Bob via estimator $\widehat{\alpha} := 1 - \frac{\left\langle \underline{\mathbf{y}}_B, \underline{\mathbf{x}}_B\right\rangle}{nP}$. Then Bob computes $\underline{\mathbf{y}}_B - (1-\widehat{\alpha})\underline{\mathbf{x}}_B$ which in turn well approximates $(1-\alpha)\underline{\mathbf{x}}_A + \underline{\mathbf{s}}_\perp$. We now observe that, once James receives $\underline{\mathbf{z}}$ and instantiates his jamming vector $\underline{\mathbf{s}}$ based on $\underline{\mathbf{z}}$, the effective channel to Bob is essentially $\underline{\widetilde{\mathbf{y}}}_B = \underline{\widetilde{\mathbf{x}}}_A + \underline{\mathbf{s}}_\perp$ where $\underline{\mathbf{s}}_\perp$ is fixed, $\underline{\widetilde{\mathbf{x}}}_A := (1-\alpha)\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}_A$ is uniformly distributed in the strip $\mathcal{T} \cap \mathcal{C}_A$. It turns out that $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{s}}_\perp$ are almost orthogonal w.h.p. Let $\widetilde{P} := (1-\alpha)^2 P$. Assuming James used up all his power (which is the worst case for Bob), let $\widetilde{N} := N - 2\alpha^2 P$. For any $\mathcal{A} \subset \mathbb{R}^n$, let $\widetilde{\mathcal{A}}$ denote $(1-\alpha)\mathcal{A}$. One can compute the *typical* radius of the decoding region induced by $\underline{\widetilde{\mathbf{x}}}_A \in \widetilde{\mathcal{T}} \cap \widetilde{\mathcal{C}}_A$ under the translation of $\underline{\mathbf{s}}_\perp$, which turns out to be approximately $\sqrt{n\frac{\widetilde{P}\widetilde{N}}{\widetilde{P}+\widetilde{N}}}$. Now invoking techniques in [21] allows us to show that as long as $\widetilde{\Lambda}$ is $(\widetilde{N}, L)$ list-decodable with constant (independent of n) list size L, then $\mathcal{C}_A$ is uniquely decodable with proba-

[2] Here $\mathcal{B}^n\left(\underline{u}, r\right)$ denotes an n-dimensional Euclidean ball centered around $\underline{u}$ of radius r.

[3] See Appendix A of [1] for preliminaries on Construction-A lattices and pertinent definitions, e.g., covering/packing radius, etc.

[4] Since scaling does not affect covering-goodness, with slight abuse of notation, we use the same Λ to denote the scaled lattice.

[5] It suffices to take $q = \mathcal{O}(1/\beta)$ and $k = \mathcal{O}(n/\log\frac{1}{\beta})$.

[6] The rate of a code $\mathcal{C}$ is defined as $R(\mathcal{C}) := \frac{\log|\mathcal{C}|}{n}$.

bility $1-2^{-2^{\Omega(n)}}$ over expurgation. Hence the $(\widetilde{P},\widetilde{N})$-list-decoding capacity $\frac{1}{2}\log\left(\frac{\widetilde{P}}{\widetilde{P}\widetilde{N}/(\widetilde{P}+\widetilde{N})}\right)=\frac{1}{2}\log\left(1+\frac{\widetilde{P}}{\widetilde{N}}\right)$ can be achieved. Minimizing over James' choice of α subject to $|\alpha|\leqslant\sqrt{\frac{N}{2P}}$ gives that under the worst jamming strategy that James can impose, the rate $\frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{N}\right)$ can be achieved. (The maximizer α^* turns out to be $\frac{N}{2P}$.) This optimization problem coincides with the one that shows up in our converse.

6) Some key lemmas: We first show that the sum of two independently and uniformly chosen codewords from $\mathcal{C}$ lies in a thin shell of radius $\sqrt{2nP}$. We call this the *typical sumset* of the lattice code.

Lemma 8. *Let $\underline{\mathbf{x}}_A,\underline{\mathbf{x}}_B$ be random lattice points sampled uniformly and independently from $\mathcal{C}$. Let $\underline{\mathbf{z}}:=\underline{\mathbf{x}}_A+\underline{\mathbf{x}}_B$. For any constant $\delta\in(0,1)$, we have*

$$\Pr_{\underline{\mathbf{x}}_A,\underline{\mathbf{x}}_B\overset{i.i.d.}{\sim}\mathcal{C}}\left[\|\underline{\mathbf{z}}\|_2\notin\sqrt{2nP(1\pm\delta)}\right]\leqslant 4\left(\frac{\sqrt{P(1-\delta^2/4)}+\sqrt{\omega}}{\sqrt{P}-\sqrt{\omega}}\right)^n.$$

We call $\underline{z}\in\mathcal{C}+\mathcal{C}$ *typical* if $\|\underline{z}\|_2\in\sqrt{2nP(1\pm\delta)}$. We also show that James is sufficiently confused, in the sense that the number of pairs of $(\underline{x}_A,\underline{x}_B)$ that sum to a received vector in the typical sumset is large.

Lemma 9. *For any $\underline{z}\in\mathcal{C}+\mathcal{C}$ in typical sumset, we have that $|\{(\underline{x}_A,\underline{x}_B)\in\mathcal{C}\times\mathcal{C}\colon\underline{x}_A+\underline{x}_B=\underline{z}\}|\geqslant C_1\cdot 2^{\frac{n}{2}\left(\log(P/2-c_{\omega,\delta})+\log\frac{1}{\tau}\right)}$, where $C_1=C_1(P)$ and $c_{\omega,\delta}$ are positive constants where $c_{\omega,\delta}\xrightarrow{\omega,\delta\to 0}0$.*

A key idea in the proof is to decompose the jamming sequence $\underline{s}$ in directions along and orthogonal to $\underline{\mathbf{z}}$. We show that

Lemma 10. *Fix $\underline{s}\in\mathcal{S}^{n-1}\left(\underline{0},\sqrt{nN}\right)$. Let $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}_B$ be two random lattice points independently and uniformly sampled from $\mathcal{C}$. Let $\underline{\mathbf{z}}:=\underline{\mathbf{x}}_A+\underline{\mathbf{x}}_B$ and $\underline{\mathbf{s}}_\perp:=\mathrm{proj}_{\underline{\mathbf{z}}^\perp}(\underline{s})$. Then the norm of $\underline{\mathbf{s}}_\perp$ is concentrated around $\sqrt{n(N-2\alpha^2P)}$ w.h.p. Specifically, for any $\delta\in(0,1)$,*

$$\Pr_{\underline{\mathbf{x}}_A,\underline{\mathbf{x}}_B\overset{i.i.d.}{\sim}\mathcal{C}}\left[\|\underline{\mathbf{s}}_\perp\|_2\notin\sqrt{n(N-2\alpha^2P(1\pm\delta))}\right]$$
$$\leqslant 4\left(\frac{\sqrt{P(1-\delta^2/4)}+\sqrt{\omega}}{\sqrt{P}-\sqrt{\omega}}\right)^n.$$

Combined with volume concentration phenomenon in high dimensions, the above lemmas imply that for any vector in the typical sumset, most pairs of codewords that sum to this vector respectively lie in a thin strip $\mathcal{T}$ of radius approximately $\sqrt{nP/2}$. It also follows that pairs of codewords from $\mathcal{T}$ that are consistent with $\underline{z}$ are approximately orthogonal to each other and have norm close to $\sqrt{nP}$. Furthermore, since a random codewords in $\mathcal{T}$ is almost isotropically distributed, it is approximately orthogonal to any $\underline{\mathbf{s}}_\perp$ w.h.p.

For this effective channel from $\underline{\widetilde{\mathbf{x}}}_A$ to $\underline{\widetilde{\mathbf{y}}}_B$, the (normalized) *average* (over $\underline{\widetilde{\mathbf{x}}}_A\sim\widetilde{\mathcal{T}}\cap\widetilde{\mathcal{C}}_A$) effective decoding radius $\mathbf{r}$ under $\underline{\mathbf{s}}_\perp$ (which corresponds to the radius $\sqrt{n}\mathbf{r}$ of the smallest ball that contains $\mathcal{B}^n(\underline{0},\sqrt{nP})\cap\mathcal{B}^n(\underline{\widetilde{\mathbf{y}}}_B,\|\underline{\mathbf{s}}_\perp\|_2))$ is shown to be approximately equal to $\frac{\widetilde{P}\widetilde{N}}{\widetilde{P}+\widetilde{N}}$ w.h.p. (over $\underline{\widetilde{\mathbf{x}}}_A\sim\widetilde{\mathcal{T}}\cap\widetilde{\mathcal{C}}_A$).

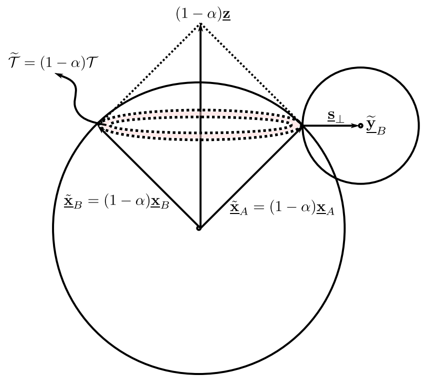
$(1-\alpha)\underline{\mathbf{z}}$
$\widetilde{\mathcal{T}}=(1-\alpha)\mathcal{T}$
$\underline{\mathbf{s}}_\perp$
$\underline{\widetilde{\mathbf{y}}}_B$
$\underline{\tilde{\mathbf{x}}}_B=(1-\alpha)\underline{\mathbf{x}}_B$
$\underline{\tilde{\mathbf{x}}}_A=(1-\alpha)\underline{\mathbf{x}}_A$

Fig. 2: The transmitted codewords $\underline{\mathbf{x}}_A$ and $\underline{\mathbf{x}}_B$ are approximately orthogonal to each other, and to $\underline{\mathbf{z}}$ w.h.p. Conditioned on $\underline{\mathbf{z}}$, $\underline{\mathbf{x}}_A$ is uniformly distributed in a thin strip (shown in pink in the figure). For any attack vector that James chooses, the effective decoding ball makes a small intersection with $\mathcal{B}^n(\underline{0},\sqrt{nP})$.

Lemma 11. *Fix any typical $\underline{z}\in\mathcal{C}+\mathcal{C}$. Fix $\underline{s}\in\mathcal{S}^{n-1}\left(\underline{0},\sqrt{nN}\right)$. Then Bob's estimate of the (normalized) average effective decoding radius $\mathbf{r}$ is concentrated around the underlying typical value $\frac{\widetilde{P}\widetilde{N}}{\widetilde{P}+\widetilde{N}}$, i.e., $\mathbf{r}\in\frac{\widetilde{P}\widetilde{N}}{\widetilde{P}+\widetilde{N}}\pm\nu$ for some arbitrarily small constant $\nu>0$.*

7) Completing the proof: Since the expurgation factor γ is sufficiently small, all above lemmas continue to hold with probability $1-2^{-2^{\Omega(n)}}$ after expurgation. Let $\mathcal{T}_{\text{good}}$ ($\mathcal{T}_{\text{bad}}:=\mathcal{T}\backslash\mathcal{T}_{\text{good}}$) denote the subset of $\mathcal{T}$ in which codewords induce typical (atypical) radii of decoding regions under $\underline{\mathbf{s}}_\perp$ assuming these codewords were transmitted. The probability that the transmitted $\underline{\mathbf{x}}_A$ falls into $\mathcal{T}_{\text{bad}}$ is exponentially small. For any of those $\underline{\mathbf{x}}_A$ in $\mathcal{T}_{\text{good}}\cap\Lambda$, by list decodability, the number of codewords in a ball centered around $\underline{\widetilde{\mathbf{x}}}_A$ of radius $\sqrt{n\widetilde{N}}$ is at most a constant L. After expurgation (with probability $1-2^{-\gamma n}$), in expectation, the number of codewords in the decoding ball is at most $L2^{-\gamma n}$. To get doubly exponential concentration (which admits a union bound over exponentially $\underline{s}\in\mathcal{B}^n\left(\underline{0},\sqrt{nN}\right)$[7]), we invoke McDiarmid's inequality and show that with probability $1-2^{-2^{\Omega(n)}}$ over expurgation, the fraction of codewords in $\mathcal{T}_{\text{good}}$ that suffer decoding errors (i.e., there exists another codeword in the decoding ball) is exponentially small, or, in $1-2^{-\Omega(n)}$ fraction of decoding balls induced by codewords in $\mathcal{T}_{\text{good}}$, there will be no codeword other than the transmitted one that survived the expurgation. The analysis is similar to that in [21].

8) Final remark: We do not believe that our bound $R=\frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{N}\right)$ is the capacity for *all* SNRs. One of our converse (Lemma 7) shows that the capacity is 0 if $\mathsf{SNR}\leqslant 4/3$ at which R is positive. We suspect that C is strictly less than R for small SNRs. Understanding the behaviour of capacity in the low-rate regime remains an intriguing open question.

[7] Here we need to quantize $\underline{s}$ using a covering/net for $\mathcal{B}^n\left(\underline{0},\sqrt{nN}\right)$ of exponential size.

References

[1] Y. Zhang, S. Vatedka, and S. Jaggi, "Quadratically constrained two-way adversarial channels," *preprint https://arxiv.org/abs/2001.02575*, 2019.

[2] D. Blackwell, L. Breiman, and A. J. Thomasian, "The Capacity of a Class of Channels under Random Coding," *Ann. of Mathematical Statistics*, vol. 31, no. 3, pp. 558–567, 1960.

[3] N. Blachman, "On the capacity of bandlimited channel perturbed by statistically dependent interference," *IRE Transactions on Information Theory*, vol. 8, pp. 48–55, 1962.

[4] B. Hughes and P. Narayan, "Gaussian arbitrarily varying channels," *IEEE Trans. Inf. Theory*, vol. 33, pp. 267–284, 1987.

[5] I. Csiszár and P. Narayan, "Capacity of the Gaussian Arbitrarily Varying Channel," *IEEE Trans. Inf. Theory*, vol. 37, pp. 18–26, 1991.

[6] T. G. Thomas and B. Hughes, "Exponential error bounds for random codes on Gaussian arbitrarily varying channels," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 643–649, 1991.

[7] B. Hughes and P. Narayan, "The capacity of a vector Gaussian arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 34, pp. 995–1003, Sept 1988.

[8] A. Sarwate and M. Gastpar, "Randomization bounds on Gaussian arbitrarily varying channels," in *Proc. IEEE Int. Symp. Information Theory*, 2006.

[9] A. Sarwate, "An AVC perspective on Correlated Jamming," in *Proc. IEEE Int. Conf. Signal Proc. and Comm.*, (Bangalore, India), 2012.

[10] Y. Zhang, S. Vatedka, S. Jaggi, and A. D. Sarwate, "Quadratically constrained myopic adversarial channels," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 611–615, IEEE, 2018.

[11] F. Haddadpour, M. Siavoshani, M. Bakshi, and S. Jaggi, "On AVCs with Quadratic Constraints," *IEEE International Symposium on Information Theory*, 2013.

[12] M. Médard, "Capacity of Correlated Jamming Channels," in *Proc. Allerton Annual Conf. on Comm., Control and Computing*, (Allerton, USA), 1997.

[13] C. Baker and I.-F. Chao, "Information capacity of channels with partially unknown noise. I. finite-dimensional channels," *SIAM Journal on Applied Mathematics*, vol. 56, pp. 946–963, 1996.

[14] S. Shafiee and S. Ulukus, "Mutual information games in multi-user channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4598–4607, 2009.

[15] F. Hosseinigoki and O. Kosut, "Capacity of the gaussian arbitrarily-varying channel with list decoding," *IEEE International Symposium on Information Theory*, 2018.

[16] Y. Zhang and S. Vatedka, "List Decoding Random Euclidean Codes and Infinite Constellations," 2019.

[17] U. Pereg and Y. Steinberg, "The capacity region of the arbitrarily varying mac: With and without constraints," *arXiv preprint arXiv:1901.00939*, 2019.

[18] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Byzantine multiple access," *arXiv preprint arXiv:1904.11925*, 2019.

[19] U. Pereg and Y. Steinberg, "The arbitrarily varying relay channel," *Entropy*, vol. 21, no. 5, p. 516, 2019.

[20] U. Pereg and Y. Steinberg, "The arbitrarily varying broadcast channel with causal side information at the encoder," *IEEE Transactions on Information Theory*, 2019.

[21] S. Jaggi and M. Langberg, "Two-way interference channels with jammers," in *Proc. IEEE Int. Symp. Information Theory*, 2017.

[22] C. J. McDonald, F. Alajaji, and S. Yuksel, "Two-way gaussian networks with a jammer and decentralized control," *IEEE Transactions on Control of Network Systems*, 2019.

[23] Y. Zhang, S. Vatedka, S. Jaggi, and A. Sarwate, "Quadratically Constrained Myopic Adversarial Channels," 2018.

[24] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3401–3416, 2005.

[25] Y. Zhang and S. Vatedka, "List decoding random euclidean codes and infinite constellations," in *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 1627–1631, July 2019.