On the Single-Slot Capacity of Random Access Over a Gaussian MAC

Onkar Dabeer
School of Technology and Computer Science
Tata Institute of Fundamental Research
Colaba, Mumbai 400 005
India
Email: onkar@tcs.tifr.res.in

***Abstract*— Consider a Gaussian multiple access channel (MAC) with two users, which do not always have a message to transmit. Neither user knows if the other is transmitting or not. Each user has two possible achievable rates depending on whether the other user is transmitting or not. Hence, in general, any coding scheme is characterized by a 4-tuple of rates. For given power constraints, we prove inner and outer bounds to the (4-dimensional) capacity region.**

I. Introduction

Consider the uplink of a wireless LAN (WLAN). There are several users associated with the access point (AP) and each has an independent, bursty source of information packets to be sent to the AP via a multiple access channel (MAC). Assuming that the time is slotted, in any given slot only a (random) subset of the users may have a packet to transmit. Moreover, a given user does not know how many other users have packets to transmit in the given slot. Thus within a slot, we are naturally led to a MAC with unknown number of transmitters. This uplink model is not new. Gallager suggested the need for such a model in [1]. Subsequently, several authors have studied the L-out-of-K (LOOK) channel (see Alsugair and Cheng [2] for more details). In the LOOK channel, exactly L out of a set of K users transmit. This channel is a special case of the normal channel network in [3, pp. 300] and its capacity is known ([2]). In general, however, the number of active users is also not known. In this context, *opportunistic* coding schemes that provide more throughput if fewer users transmit simultaneously are desirable. For example, [4] considers the two user Gaussian MAC where each user independently has a message to transmit with some probability, and it proposes opportunistic codes based on the ideas of superposition coding and rate splitting. While [4] provides an achievable region, the precise capacity region for this problem seems to be unknown. In this paper, we prove inner and outer bounds to the capacity region in terms of auxiliary random variables (see Theorem 1, 2, Section III).

The paper is organized as follows. In Section II, we describe the precise notion of achievability used in this paper and define various regions used to inner bound and outer bound the capacity region. The main results are stated and proved in Section III. The conclusion is given in Section IV.

II. Basic Setup

Consider a Gaussian MAC channel with a maximum of two users. The two users may not always have a messages to transmit, and it is likely that none of them transmit, or only one of them transmits, or they both transmit. Neither user knows if the other will transmit or not. But we assume that the receiver knows which users have transmitted. (We note that this information can be communicated to the receiver at zero rate and the capacity region remains unchanged even if this assumption is not made.) We are interested in opportunistic codes where the users get a lower rate when they collide, and a higher rate when they do not collide. This is made precise in the following paragraphs.

Consider the three channels:

$$Z_t = X_t + Y_t + W_t, \quad t = 1, ..., n \quad \text{(Gaussian MAC)} \tag{1}$$
$$Z_t = X_t + W_t, \quad t = 1, ..., n \quad \text{(Gaussian channel)} \tag{2}$$
$$Z_t = Y_t + W_t, \quad t = 1, ..., n \quad \text{(Gaussian channel).} \tag{3}$$

Here X^n, Y^n are the codewords of user 1 and 2 respectively. We assume that the noise sequence $\{W_t\}$ is i.i.d. $\mathcal{N}(0, \sigma^2)$. The channel (1) arises when both the users transmit, channel (2) arises when only user 1 transmits and channel (3) arises when only user 2 transmits. (The case when no one transmits is not of interest.) We use E to denote the transmission events: $E = i$ if only the ith user transmits and $E = (1, 2)$ if both users transmit. Even though we do not need the probability law of E in this paper, it is convenient to think of E as a random variable independent of the other random variables here.

Remark: In WLANs, even if a user has a message to transmit, it may not transmit depending upon recent history. In this paper, we do not consider this issue and only study the single-slot capacity region conditioned on the various transmission events.

Let $M_1 = [M_{10}, M'_{11}]$ be the message of user 1 and $M_2 = [M_{20}, M'_{22}]$ be the message of user 2. When both the users transmit, we want to convey the message (M_{10}, M_{20}) reliably over the channel (1). When only user i transmits, we want the entire message M_i to be conveyed reliably. As is usual, the number of messages grows exponentially with the block-length n and our interest is in identifying the rate vectors $(R_{10}, R_{20}, R_1, R_2)$ such that

- (R_{10}, R_{20}) is achievable on the Gaussian MAC channel, that is, when both users transmit ($E = (1, 2)$).
- R_i is achievable when only user i transmits. Clearly we have $R_i \geq R_{i0}$ and we assume so throughout.

The definition of "achievability" in this setting is stated below. We begin by introducing some more notation.

Let P_i be the power constraint on user i. We represent message M_i by a binary sequence $b_i^{nR_i} = [b_{i,1}, ..., b_{i,nR_i}]$. We assume that all messages are equally likely. The first nR_{i0} bits $b_i^{nR_{i0}}$ correspond to message M_{i0}. Let

$$f_i^{(n)} : \{0,1\}^{nR_i} \to \mathbb{R}^n, \quad i = 1, 2$$

be the encoders with block-length n, and let $g_{i,E}^{(n)}$ be the decoder of user i under event E. We denote the decoded message bits by $\hat{b}_{i,\cdot}$.

Definition: The 4-tuple $\boldsymbol{R} = (R_{10}, R_{20}, R_1, R_2)$ is said to be *achievable* under a power constraint (P_1, P_2) if there exists a sequence of codes of block length n such that

1) **Power constraints:**
$$\frac{1}{n}\sum_{t=1}^{n} X_t^2 \leq P_1, \quad \frac{1}{n}\sum_{t=1}^{n} Y_t^2 \leq P_2.$$
2) **Achievability when only user i transmits, $i = 1, 2$:**
$$P\left(\hat{b}_i^{nR_i} \neq b_i^{nR_i} \middle| \text{ Only user } i \text{ transmits}\right) \to 0 \text{ as } n \to \infty.$$
3) **Achievability when both users transmit:**
$$P\left(\hat{b}_1^{nR_{10}} \neq b_1^{nR_{10}} \text{ or } \hat{b}_2^{nR_{20}} \neq b_2^{nR_{20}} \middle| \text{ Both transmit}\right) \to 0 \text{ as } n \to \infty.$$

Remark: As per the above definition, the transmitter does not know the exact number of bits correctly received at the receiver. In a real system, a feedback mechanism is needed to convey this information to the transmitter.

Definition: The *achievable rate region* is the closure of the set of achievable rates and is denoted by $\mathcal{C}(P_1, P_2)$.

Definition: The rate-power vector $(\boldsymbol{R}, Q_1, Q_2) \in (\mathbb{R}^+)^6$ is said to be *directly achievable* if there are random variables U, V, X, Y, Z such that Z is the channel output (of the channel corresponding to event E) with inputs X, Y, and,

$$\begin{aligned} R_{10} &< I(U; Z|V) \\ R_{20} &< I(V; Z|U) \\ R_{10} + R_{20} &< I(U, V; Z) \\ R_1 - R_{10} &< I(X; Z|U) \\ R_2 - R_{20} &< I(Y; Z|V) \end{aligned} \tag{4}$$

and

$$\begin{aligned} &U \text{ and } V \text{ are independent} \\ &X \text{ and } Y \text{ are independent} \\ &U \to X \to Z \text{ given } E = 1 \\ &V \to Y \to Z \text{ given } E = 2 \\ &(U, V) \to (X, Y) \to Z \text{ given } E = (1, 2) \\ &E[X^2] \leq Q_1, E[Y^2] \leq Q_2. \end{aligned} \tag{5}$$

We denote the directly achievable rate-power region by $\mathcal{D}$.

To establish an outer bound, we define region $\mathcal{D}_2$ below.
Definition: The rate-power vector $(\boldsymbol{R}, Q_1, Q_2) \in \mathcal{D}_2$ if there are random variables $U, V, \tilde{U}, \tilde{V}, X, Y$ such that Z is the channel output (of the channel corresponding to event E) with inputs X, Y, and,

$$\begin{aligned} R_{10} &< I(U; Z|\tilde{V}) \\ R_{20} &< I(V; Z|\tilde{U}) \\ R_{10} + R_{20} &< I(U, V; Z) \\ R_1 - R_{10} &< I(X; Z|\tilde{U}) \\ R_2 - R_{20} &< I(Y; Z|\tilde{V}) \end{aligned} \tag{6}$$

and

$$\begin{aligned} &U \text{ and } V \text{ are independent} \\ &X \text{ and } Y \text{ are independent} \\ &\tilde{U} \to U \to X \to Z \text{ given } E = 1 \\ &\tilde{V} \to V \to Y \to Z \text{ given } E = 2 \\ &(\tilde{U}, \tilde{V}) \to (U, V) \to (X, Y) \to Z \text{ given } E = (1, 2) \\ &E[X^2] \leq Q_1, E[Y^2] \leq Q_2. \end{aligned} \tag{7}$$

We note that $\mathcal{D} \subset \mathcal{D}_2$.

III. Main Results

The following result gives an inner bound for the achievable rate region in terms of the directly achievable rate region. (A possible improvement to this bound is suggested towards the end of the section.)

Theorem 1:
$$\left\{\boldsymbol{R} : (\boldsymbol{R}, P_1, P_2) \in \text{ conv.cl}(\mathcal{D})\right\} \subset \mathcal{C}(P_1, P_2) \tag{8}$$
where $\in$ conv.cl($\mathcal{D}$) is the convex closure of $\mathcal{D}$.

Proof: The proof is based on standard arguments for the MAC and broadcast channel [5]. Hence we skip the details and only give an outline below.

First we show that $(\boldsymbol{R}, Q_1, Q_2) \in \mathcal{D}$ is achievable when the power constraints are Q_1, Q_2. Let U, V, X, Y, Z be random variables that satisfy the conditions (4), (5) for $(\boldsymbol{R}, Q_1, Q_2)$ to be in $\mathcal{D}$. The proof follows random coding arguments using these random variables and the ensemble of codes used by each of the users is similar to that for a degraded broadcast channel [5]. At encoder 1, first $2^{nR_{10}}$ sequences U^n are generated in i.i.d. fashion using the law of U. These U^n sequences serve as 'cloud centers,' and for each cloud center, $2^{n(R_1 - R_{10})}$ codewords are generated independently, yielding a total of 2^{nR_1} codewords. The n symbols in a codeword are generated independently and at time t, the symbol is generated using the conditional law of X given that $U = u_t$, where u_t is the t^{th} symbol in the cloud center. Given a message $M_1 = b_1^{nR_1}$, the first nR_{10} bits (message M_{10}) are used to choose a U^n sequence, and the remaining bits (message M_{20}) are used to choose a codeword from the cloud of the chosen U^n sequence. Similarly the code ensemble at user 2 is obtained from V^n and Y^n.

Consider first $E = (1, 2)$. The effective MAC between (U^n, V^n) and Z^n can be checked to be memoryless. It follows from standard techniques for the MAC that any rates satisfying

$$\begin{aligned} R_{10} &< I(U; Z|V) \\ R_{20} &< I(V; Z|U) \\ R_{10} + R_{20} &< I(U, V; Z) \end{aligned} \tag{9}$$

are achievable.

Now consider $E = i$. In this case, the superposition code is decoded like for a degraded broadcast channel [5]. (Here the message M_{i0} corresponds to the message of the 'degraded user.') Thus we get that if $R_1 < R_{10} + I(X; Z|U)$, where R_{10}, R_{20} satisfy the MAC bounds above, then it is achievable. A similar result holds for R_2.

Thus we have shown that $(\boldsymbol{R}, Q_1, Q_2)$ is achievable. Now suppose we are given $(\boldsymbol{R}, P_1, P_2) \in$ conv($\mathcal{D}$). By Caratheodory's theorem [5, pp. 398], we know that any point in conv($\mathcal{D}$) can be written as a convex combination of 8 or less points in $\mathcal{D}$. Time sharing of the schemes corresponding to these 8 points then yields that points in conv($\mathcal{D}$) are achievable. Since the points in the closure of a set can be approached by a sequence of points in the set, the result is proved. ∎

We next establish an outer bound for the capacity region.

Theorem 2:

$$\mathcal{C}(P_1, P_2) \subset \Big\{\boldsymbol{R} : (\boldsymbol{R}, P_1, P_2) \in \text{ conv.cl}(\mathcal{D}_2)\Big\} \tag{10}$$

where $\in$ conv.cl$(\mathcal{D}_2)$ is the convex closure of $\mathcal{D}_2$.

Proof: First consider the case when $E = (1, 2)$. Since M_1 and M_2 are independent

$$\begin{aligned} I(M_{10}; Z^n) &\leq I(M_{10}; Z^n|M_{20}) \\ &= \sum_{t=1}^{n} I(M_{10}; Z_t|M_{20}, Z^{t-1}) \end{aligned}$$

where we used the chain rule in the second step. This gives

$$\begin{aligned} &I(M_{10}; Z^n) \\ &\leq \sum_{t=1}^{n} \Big[H(Z_t|M_{20}, Z^{t-1}) - H(Z_t|M_{10}, M_{20}, Z^{t-1})\Big] \\ &\leq \sum_{t=1}^{n} \Big[H(Z_t|M_{20}, Z^{t-1}) - H(Z_t|M_{10}, M_{20}, X^{t-1}, Z^{t-1})\Big] \\ &\quad = \sum_{t=1}^{n} I(U_t; Z_t|\tilde{V}_t) \end{aligned}$$

where

$$U_t := (M_{10}, X^{t-1}), \quad \tilde{V}_t := (M_{20}, Z^{t-1}).$$

Using this and Fano's inequality when $E = (1, 2)$, we get that

$$\begin{aligned} nR_{10} = H(M_{10}) &= I(M_{10}; Z^n) + H(M_{10}|Z^n) \\ &\leq \sum_{t=1}^{n} I(U_t; Z_t|\tilde{V}_t) + o(n). \end{aligned}$$

Similar bound holds for nR_{20} and we get

$$\begin{aligned} R_{10} &\leq \frac{1}{n}\sum_{t=1}^{n} I(U_t; Z_{0,t}|\tilde{V}_t) + o(1), \\ R_{20} &\leq \frac{1}{n}\sum_{t=1}^{n} I(V_t; Z_{0,t}|\tilde{U}_t) + o(1) \end{aligned} \tag{11}$$

where

$$V_t := (M_{20}, Y^{t-1}), \quad \tilde{U}_t := (M_{10}, Z^{t-1}).$$

Next we bound the sum-rate. Again by Fano's inequality

$$\begin{aligned} &n(R_{10} + R_{20}) \\ &\leq I(M_{10}, M_{20}; Z^n) + o(n) \\ &\quad = \sum_{t=1}^{n} I(M_{10}, M_{20}; Z_t|Z^{t-1}) + o(n) \\ &\leq \sum_{t=1}^{n} \left[H(Z_t) - H(Z_t|M_{10}, M_{20}, Z^{t-1})\right]. \end{aligned}$$

Since $Z^{t-1} = X^{t-1} + Y^{t-1} + W^{t-1}$ and $\{W_t\}$ are i.i.d.,

$$Z^{t-1} \to (X^{t-1}, Y^{t-1}) \to Z_t \text{ given } M_{10}, M_{20}.$$

Therefore by applying the data processing inequality

$$\begin{aligned} &n(R_{10} + R_{20}) \\ &\leq \sum_{t=1}^{n} \left[H(Z_t) - H(Z_{0,t}|M_{10}, M_{20}, X^{t-1}, Y^{t-1})\right]. \end{aligned}$$

Hence

$$R_{10} + R_{20} \leq \frac{1}{n}\sum_{t=1}^{n} I(U_t, V_t; Z_t) + o(1). \tag{12}$$

Consider now the event $E = 1$. We next bound R_1. Since all messages are equally likely

$$\begin{aligned} nR_1 = H(M_1) &= H(M_{10}, M'_{11}) \\ &= nR_{10} + I(M'_{11}; Z^n) + H(M'_{11}|Z^n). \end{aligned}$$

Applying Fano's inequality, and then using the fact that M_{10} and M'_{11} are independent, we get

$$n(R_1 - R_{10}) = I(M'_{11}; Z^n) + o(n) \leq I(M'_{11}; Z^n|M_{10}) + o(n).$$

Application of the data-processing inequality and the chain rule then gives

$$
\begin{aligned}
n(R_1 - R_{10}) &\le I(X^n; Z^n | M_{10}) + o(n) \\
&= \sum_{t=1}^{n} I(X^n; Z_t | M_{10}, Z^{t-1}) + o(n) \\
&= \sum_{t=1}^{n} \Big[H(Z_t | M_{10}, Z^{t-1}) \\
&\quad - H(Z_t | M_{10}, Z^{t-1}, X^n) \Big] + o(n).
\end{aligned}
$$

When $E = 1$, given X_t, Z_t is independent of X^{t-1} and X_{t+1}^n. Therefore

$$
\begin{aligned}
n(R_1 - R_{10}) &\le \sum_{t=1}^{n} \Big[H(Z_t | M_{10}, Z^{t-1}) \\
&\quad - H(Z_t | M_{10}, Z^{t-1}, X_t) \Big] + o(n) \\
\therefore R_1 - R_{10} &\le \frac{1}{n} \sum_{t=1}^{n} I(X_t; Z_t | \tilde{U}_t) + o(1). \qquad (13)
\end{aligned}
$$

Similarly, when $E = 2$,

$$
R_2 - R_{20} \le \frac{1}{n} \sum_{t=1}^{n} I(Y_t; Z_t | \tilde{V}_t) + o(1). \qquad (14)
$$

The random variables

$$
U_t, V_t, \tilde{U}_t, \tilde{V}_t, X_t, Y_t, Z_t
$$

satisfy the conditions (6) and (7). Moreover the codewords satisfy the power constraints,

$$
\frac{1}{n} \sum_{t=1}^{n} E[X_t^2] \le P_1, \quad \frac{1}{n} \sum_{t=1}^{n} E[Y_t^2] \le P_2.
$$

This implies that $\boldsymbol{R}$ is such that $(\boldsymbol{R}, P_1, P_2)$ is in the convex closure of $\mathcal{D}_2$. This completes the proof.

Remark: We note that the inner bound is based on superposition coding with two *layers* while the outer bound suggests a three-layer superposition code. It is possible to establish inner bounds using three layer superposition codes, but we have been unable to close the gap to the outer bound.

IV. Conclusion

We prove inner and outer bounds for the capacity region of single-slot random access over Gaussian MAC. There is further scope to improve the gap between these bounds, particularly in the high SNR case. The removal of the auxiliary random variables in these bounds appears to be a challenging problem.

Acknowledgement

This work was supported by Grant 13(10)/2006-CC&BT from the Ministry of Communications and Information Technology, Government of India.

References

[1] R. Gallager, "A perspective on multiaccess channels," *IEEE Transactions on Information Theory*, vol. 31, no. 2, pp. 124–142, March 1985.

[2] A. Alsugair and R. Cheng, "Symmetric Capacity and Signal Design for L-out-of-K Symbol-Synchronous CDMA Gaussian Channels," *IEEE Transactions on Information Theory*, vol. 41, no. 4, pp. 1072–1082, July 1995.

[3] I. Csiszar and J. Korner, *Information theory*, Akademiai Kiado, Budapest, 1981.

[4] M. Medard et al., "Capacity of Time-Slotted ALOHA Packetized Multiple-Access Systems Over the AWGN Channel," *IEEE Transactions on Wireless Communications*, vol. 3, no. 2, pp. 486–499, March 2004.

[5] T. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, New York, 1991.