

Zero Error Strategic Communication

Anuj S. Vora

Systems and Control Engineering Department
Indian Institute of Technology, Bombay
Mumbai, 400076, India
Email: anujvora@iitb.ac.in

Ankur A. Kulkarni

Systems and Control Engineering Department
Indian Institute of Technology, Bombay
Mumbai, 400076, India
Email: kulkarni.ankur@iitb.ac.in

Abstract—We introduce a new setting in information theory where a receiver tries to exactly recover a source signal from a *dishonest* sender who sends messages with an intention to maximize its utility. The sender can send messages to the receiver over a noiseless channel whose input space is the entire signal space, but due to its dishonesty, not all signals can be recovered. We formulate the problem as a game between the sender and the receiver, where the receiver chooses a strategy such that it can recover the maximum number of source signals. We show that, despite the strategic nature of the sender, the receiver can recover an exponentially large number of signals. We show that this maximum rate of strategic communication is lower bounded by the independence number of a suitably defined graph on the alphabet and upper bounded by the Shannon capacity of this graph. This allows us to exactly characterize the rate of strategic communication for perfect graphs.

I. INTRODUCTION

We introduce a new setting in information theory with a sender and a receiver, where the receiver is trying to exactly recover a sequence of source symbols privately known to a sender. The sender can convey information about the signal by sending a message to the receiver via a noiseless channel of unit rate. The sender, however, is trying to maximize its utility and may have an incentive to misreport its information. The receiver now has to decode the true signal from the message sent by the sender. We ask the following question: given that the sender is a dishonest reporter, what is the maximum number of signals that can be recovered by the receiver?

This unconventional setting between a sender and a receiver is important in networked control systems such as IoT and smart grids. These systems comprise of multiple entities like sensors, controllers and smart devices, that are remotely connected via communication channels. In a typical scenario, a sender such as a fusion center collects information observed by the sensors and transmits it via a communication channel to a controller. The controller then takes appropriate action to achieve a certain objective. However, such networked systems are vulnerable to adversarial attacks which may cause the sender to act maliciously and misrepresent its information. These networked systems form the backbone of critical systems and their failure could be catastrophic. Thus, it is of utmost importance to study this problem and determine the *strategies* of the receiver which ensure communication with the sender.

This setting is unlike the information-theoretic problems of communication where the sender and receiver have a common aim of communication. In our setting, the sender can mislead the receiver for its personal gains. The receiver, thus, has to

strategize to extract truthful information from the sender. We show that, barring the case when the sender is a pathological liar, i.e., it speaks anything but the truth, the receiver can recover an *exponentially* large number of signals.

We formulate the communication problem as a game between the sender and the receiver, where the sender acts to maximize its utility and the receiver aims to maximize the number of signals it can recover exactly. We consider a block setting, where the sender observes a sequence of source symbols, which it can convey to the receiver by sending a message through a noiseless channel. The receiver then has to *decode* this message and recover the true information. We consider a leader-follower setting for our problem, where the receiver is the leader and declares its decoding strategy before the sender chooses its mapping. We then define a *strategic graph* on the source sequences, which is induced by the utility of the sender, and where two source sequences are connected via an edge if they can be confused by the receiver. We show that, in equilibrium, the receiver effectively recovers the largest independent set of the strategic graph. We define a notion of the *strategic capacity* of the graph and the *rate of strategic communication*. Our main result shows that the capacity is lower bounded by the independence number of a base graph and upper bounded by the Shannon capacity of the base graph.

The Shannon capacity is computed by considering the strong product of the *confusability graph* induced by a noisy channel [1]. We show that constructing a similar graph by taking n -fold strong product of the base graph induced by the utility, we only get a subgraph of the strategic graph. Thus, the Shannon capacity of the strategic graph is an upper bound on the strategic capacity. The capacities are equal in the case of perfect graphs since the capacity of a perfect graph is the independence number of the graph. To the best of our knowledge, the strategic capacity we introduce is the first case of a quantity that lies between the independence number and the Shannon capacity.

While the strategic communication problem is not a standard communication problem, it does have traces of both channel coding as well as source coding. The strategic nature of the sender is akin to the ambiguity of the channel output and the noiseless medium is analogous to the noise-free transmission in source coding. The strategic capacity essentially captures the idea that to communicate with a *noisy* sender, the receiver has to perform a *compression* of the source.

The problem of communication where the sender and receiver have misaligned objectives has been studied in various forms in [2], [3], [4], [5]. The Shannon graph capacity problem has been extensively studied [6]. However, determining the

capacity for graphs as small as a 7-cycle graph is open [7].

II. PROBLEM FORMULATION

Let the string seen by the sender consist of symbols lying in a finite alphabet \mathcal{X} . We take $\mathcal{X} = \{0, 1, \dots, q-1\}$ with $q = |\mathcal{X}|$. A generic graph is denoted as $G = (V, E)$ where V is the set of vertices and E is the set of edges. When two vertices x and y are connected via an edge, we denote it either as $(x, y) \in E$ or as $x \sim y$. The size of the largest independent set of a graph G is denoted as $\alpha(G)$. We denote $\mathcal{I}(G)$ as the collection of all independent sets of the graph G .

Consider a setting with a sender and a receiver, where the sender observes a sequence of source signals $X^n = (X_1, \dots, X_n) \in \mathcal{X}^n$, where X_i are generated randomly according to some distribution. The receiver wishes to perfectly recover this sequence from the sender. As the receiver aims for perfect recovery, we do not assume any specific distribution for X_i . The sender can convey information about its source by transmitting a message as $s_n(X^n) = Y^n$, where $s_n : \mathcal{X}^n \rightarrow \mathcal{X}^n$. The message is noiselessly relayed to the receiver who decodes the message as $g_n(Y^n) = \hat{X}^n$, where $g_n : \mathcal{X}^n \rightarrow \mathcal{X}^n \cup \Delta$. Here Δ is an error symbol that gives a utility of $-\infty$ to the sender and hence is never preferred by the sender. Let

$$\mathcal{D}(g_n, s_n) := \{x^n \in \mathcal{X}^n : g_n \circ s_n(x^n) = x^n\} \quad (1)$$

be the set of perfectly recovered sequences when the receiver plays g_n and the sender plays s_n . The receiver aims to maximize the size of this set by choosing a strategy g_n . The sender, on the other hand, chooses a strategy s_n to maximize the utility $u_n : \mathcal{X}^n \cup \Delta \times \mathcal{X}^n \rightarrow \mathbb{R}$ given as

$$u_n(\hat{x}^n, x^n) = \frac{1}{n} \sum_{i=1}^n u(\hat{x}_i, x_i),$$

where $u : (\mathcal{X} \cup \Delta) \times \mathcal{X} \rightarrow \mathbb{R}$. Here x^n is the sequence observed by the sender and \hat{x}^n is the sequence recovered by the receiver. Note that Δ is such that $u_n(\Delta, x^n) = \sum_{i=1}^n u(\Delta, x_i)/n$ for all $x^n \in \mathcal{X}^n$ and for all n . Further, $u(\Delta, x) = -\infty$ for all $x \in \mathcal{X}$.

We study this setting as a game between the sender and the receiver. In particular, we consider a leader-follower game, also called a *Stackelberg game*, where the receiver is the leader and the sender is the follower. We consider this formulation apt for our setting due to the following reasons. In a Stackelberg game, the leader plays its strategy before the follower and hence has an advantage in the game. Since we study a problem where the receiver tries to “extract” information from the sender, we can assume that the receiver is aware of the strategic nature of the sender and plays its strategy before the sender. For instance, in a smart grid, the regulator is aware of the incentives available to the consumers for misreporting the demand and usage data. Its objective is to appropriately regulate the load by extracting the true demand and usage data from the consumers.

The game proceeds as follows. The receiver, being the leader, plays its strategy before the sender. For a given strategy of the receiver, the sender chooses the best response that maximizes its utility. The receiver anticipates this response of the sender and accordingly chooses an optimal strategy that maximizes its objective. This leads to the equilibrium concept called the

Stackelberg equilibrium solution. Formally, the optimal strategy of the receiver is given as

$$\hat{g}_n \in \arg \max_{g_n} \min_{s_n \in \mathcal{B}(g_n)} |\mathcal{D}(g_n, s_n)|, \quad (2)$$

where the best response of the sender, $\mathcal{B}(g_n)$, is given as

$$\mathcal{B}(g_n) = \left\{ s_n : u_n(g_n \circ s_n(x^n), x^n) \geq u_n(g_n \circ s'_n(x^n), x^n) \right. \\ \left. \forall x^n \in \mathcal{X}^n, \forall s'_n \right\}. \quad (3)$$

Thus, the best response of the sender for a strategy g_n of the receiver is a collection of strategies, s_n , such that, for any observed sequence x^n , the sequence recovered by the receiver, $g_n \circ s_n(x^n)$, gives the highest utility compared to any other recovered sequence $g_n \circ s'_n(x^n)$.

In (2), the receiver minimizes over the set $\mathcal{B}(g_n)$. We incorporate this minimization because, in general, the best response of the sender may not be unique and the receiver does not have control over the choice of the sender’s best response. Thus, we assume that the receiver chooses its strategy according to the worst case scenario and hence adopts a *pessimistic* viewpoint. Alternatively, an *optimistic* receiver would maximize over $\mathcal{B}(g_n)$. We do not consider the optimistic formulation.

We assume the following structure for the utility u .

Assumption 2.1: Let u be such that

$$|u(i, i) - u(j, i)| = |u(k, k) - u(l, k)| \\ \forall i, j, k, l \in \mathcal{X}, j \neq i, k \neq l.$$

Thus all deviations from the truth contribute in equal magnitude to the benefit or loss of the sender.

We now define few notions of graphs on the space of sequences \mathcal{X}^n . First we define a graph induced by the utility.

Definition 2.1 (Strategic graph): A strategic graph, denoted as $G_n = (\mathcal{X}^n, E)$, is a graph where $(x^n, y^n) \in E$ if

$$u_n(x^n, x^n) \leq u_n(y^n, x^n) \text{ or } u_n(y^n, y^n) \leq u_n(x^n, y^n).$$

For $n = 1$, the graph induced on the alphabet \mathcal{X} is G^1 and is denoted as G . We also call this graph as the *base graph*.

Thus, two sequences have an edge in the graph G_n if the sender has an incentive to report one sequence as the other. We now define the strong product operation which will be used to construct sequence of graphs from the base graph.

Definition 2.2 (Strong product): Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs. Then the strong product of the graphs G_1, G_2 is given by a graph $G = (V, E)$ where $V = V_1 \times V_2$. Further, two vertices $(x, x'), (y, y') \in V$, with $x, y \in V_1$ and $x', y' \in V_2$, are connected by an edge if and only if one of the following holds

- $x = y$ and $x' \sim y'$
- $x \sim y$ and $x' = y'$
- $x \sim y$ and $x' \sim y'$

The strong product operation is denoted as \boxtimes and the product graph G is written as $G = G_1 \boxtimes G_2$.

Using this operation, we construct the following graphs from the base graph G .

Definition 2.3 (Product graph): A product graph denoted as G_n^{\boxtimes} is a graph constructed by taking n -fold strong product of the graph G , i.e.,

$$G_n^{\boxtimes} = G \boxtimes G \boxtimes \dots \boxtimes G.$$

For completeness, we define the notion of the subgraph.

Definition 2.4 (Subgraph): A graph $G_1 = (V_1, E_1)$ is a subgraph of $G = (V, E)$ if $V_1 \subseteq V$ and $E_1 \subseteq E$.

Definition 2.5 (Cycle graph): A graph G with $\{0, 1, \dots, q-1\}$ as the vertex set is called a q -cycle graph if two vertices i, j are connected with an edge if and only if $j = (i+1) \bmod q$.

We define the rate of strategic communication as follows.

Definition 2.6 (Rate of Strategic Communication): For any strategy g_n , the rate of strategic communication is defined as

$$R(g_n) = \min_{s_n \in \mathcal{B}(g_n)} |\mathcal{D}(g_n, s_n)|^{1/n}.$$

The perfectly decoded set $\mathcal{D}(g_n, s_n)$ is given by (1). We now define the maximum rate of strategic communication.

Definition 2.7 (Maximum Rate of Strategic Communication): Let \hat{g}_n be a sequence of equilibrium strategies and let $R(\hat{g}_n)$ be the corresponding rate of strategic communication. The maximum rate of strategic communication, denoted by \mathcal{R} , is given as

$$\mathcal{R} = \limsup_n R(\hat{g}_n).$$

III. GAME BETWEEN THE SENDER AND RECEIVER

A. Recovery of independent set in Stackelberg equilibrium

In this section, we begin the analysis of the game between the sender and receiver defined in the previous section. We determine the connection between the Stackelberg game given by (3), (2) and the independent sets of the graph G_n . We first show that, in the game, the receiver can only recover an independent set of the graph. For that, we define

$$\mathcal{S}(g_n) = \arg \min_{s_n \in \mathcal{B}(g_n)} |\mathcal{D}(g_n, s_n)|,$$

where g_n is any strategy of the receiver.

Lemma 3.1: Let $n \in \mathbb{N}$ and let G_n be the strategic graph. Consider a strategy g_n for the receiver. Then, for all strategies $s_n \in \mathcal{S}(g_n)$, $\mathcal{D}(g_n, s_n)$ is an independent set in G_n .

Proof : For strategies g_n such that $\min_{s_n \in \mathcal{S}(g_n)} |\mathcal{D}(g_n, s_n)| \leq 1$, the claim trivially holds. Let g_n be such that $|\mathcal{D}(g_n, s_n)| \geq 2 \forall s_n \in \mathcal{S}(g_n)$. We prove the claim by contradiction.

Suppose for some strategy $s_n \in \mathcal{S}(g_n)$, the set $\mathcal{D}(g_n, s_n)$ is not an independent set in G_n . Then, there exist distinct sequences $\bar{x}^n, \hat{x}^n \in \mathcal{D}(g_n, s_n)$ such that $u_n(\bar{x}^n, \bar{x}^n) \leq u_n(\hat{x}^n, \bar{x}^n)$. Using this, we define a strategy \bar{s}_n as

$$\bar{s}_n(x^n) = \begin{cases} s_n(x^n) & \forall x^n \neq \bar{x}^n \\ s_n(\hat{x}^n) & \text{for } x^n = \bar{x}^n. \end{cases}$$

Thus, \bar{s}_n is also a best response since

$$u_n(g_n \circ \bar{s}_n(x^n), x^n) = u_n(g_n \circ s_n(x^n), x^n) \quad \forall x^n \neq \bar{x}^n$$

and for $x^n = \bar{x}^n$, we get $u_n(g_n \circ \bar{s}_n(\bar{x}^n), \bar{x}^n)$

$$\begin{aligned} &= u_n(g_n \circ s_n(\hat{x}^n), \bar{x}^n) = u_n(\hat{x}^n, \bar{x}^n) \\ &\geq u_n(\bar{x}^n, \bar{x}^n) = u_n(g_n \circ s_n(\bar{x}^n), \bar{x}^n). \end{aligned} \quad (4)$$

Here (4) follows since $g_n \circ s_n(\hat{x}^n) = \hat{x}^n$. Further, $g_n \circ \bar{s}_n(\bar{x}^n) = \hat{x}^n \neq \bar{x}^n = g_n \circ s_n(\bar{x}^n)$. Thus, the sequence $\bar{x}^n \in \mathcal{D}(g_n, s_n)$ is not recovered by the pair (g_n, \bar{s}_n) and hence \bar{x}^n does not lie in $\mathcal{D}(g_n, \bar{s}_n)$. Thus, $\mathcal{D}(g_n, \bar{s}_n) \subset \mathcal{D}(g_n, s_n)$ which gives $|\mathcal{D}(g_n, \bar{s}_n)| < |\mathcal{D}(g_n, s_n)|$. However, this is a contradiction since $s_n \in \mathcal{S}(g_n)$. Thus for all $s_n \in \mathcal{S}(g_n)$, the set $\mathcal{D}(g_n, s_n)$

is an independent set in G_n . ■

In the next theorem, we show that the receiver can recover any given independent set of the graph.

Lemma 3.2: Let $n \in \mathbb{N}$ and let G_n be the strategic graph. Consider $\mathcal{I}_n \in \mathcal{S}(G_n)$ and define a strategy g_n as

$$g_n(x^n) = \begin{cases} x^n & \text{if } x^n \in \mathcal{I}_n \\ \Delta & \text{if } x^n \notin \mathcal{I}_n. \end{cases} \quad (5)$$

Then, the best response of sender, $\mathcal{B}(g_n)$, is such that

$$\mathcal{D}(g_n, s_n) = \mathcal{I}_n \quad \forall s_n \in \mathcal{B}(g_n).$$

Proof : Since Δ is never preferred by the sender, we can assume without loss of generality, that for all $s_n \in \mathcal{B}(g_n)$ and for all $x^n, g_n \circ s_n(x^n) \in \mathcal{I}_n$ and hence $\mathcal{D}(g_n, s_n) \subseteq \mathcal{I}_n$. We will now show $\mathcal{I}_n \subseteq \mathcal{D}(g_n, s_n)$ for all $s_n \in \mathcal{B}(g_n)$.

Consider an $x^n \in \mathcal{I}_n$. For any $s_n \in \mathcal{B}(g_n)$, the utility of the sender is $u_n(g_n \circ s_n(x^n), x^n) = u_n(x^n, x^n)$ for some $x'^n \in \mathcal{I}_n$. Since, \mathcal{I}_n is an independent set, we have $u_n(x'^n, x^n) < u_n(x^n, x^n)$ for all $x'^n \in \mathcal{I}_n, x'^n \neq x^n$. Thus we have, $u_n(g_n \circ s_n(x^n), x^n) \leq u_n(x^n, x^n) \quad \forall x^n \in \mathcal{I}_n$, with equality if and only if $g_n \circ s_n(x^n) = x^n$. Clearly, the optimal choice of s_n for the sender, is such that $s_n(x^n) = x^n$ for all $x^n \in \mathcal{I}_n$. In particular, all the best responses $s_n \in \mathcal{B}(g_n)$ are such that $s_n(x^n) = x^n$ for all $x^n \in \mathcal{I}_n$. Thus, for all $s_n \in \mathcal{B}(g_n)$, $\mathcal{I}_n \subseteq \mathcal{D}(g_n, s_n)$. ■

Using the above results, we show that in an equilibrium, the receiver recovers the largest independent set of the graph.

Theorem 3.3: Let $n \in \mathbb{N}$ and let G_n be the strategic graph. For all Stackelberg equilibrium strategies \hat{g}_n of the receiver,

$$R(\hat{g}_n) = \alpha(G_n)^{1/n}.$$

Proof : From Lemma 3.1, we have that for all strategies g_n , $\mathcal{D}(g_n, s_n)$ is an independent set in the graph G_n for all $s_n \in \mathcal{B}(g_n)$. Further, from Lemma 3.2, we have that for all $\mathcal{I}_n \in \mathcal{S}(G_n)$, there exists g_n such that $\mathcal{D}(g_n, s_n) = \mathcal{I}_n$ for all $s_n \in \mathcal{B}(g_n)$. Thus, we have

$$\max_{g_n} R(g_n) = \max_{\mathcal{I}_n \in \mathcal{S}(G_n)} |\mathcal{I}_n|^{1/n} = \alpha(G_n)^{1/n}. \quad \blacksquare$$

Using this theorem, we can quantify the maximum rate of strategic communication.

Theorem 3.4: Let $\{G_n\}_{n \geq 1}$ be the sequence of strategic graphs. The maximum rate of strategic communication is

$$\mathcal{R} = \limsup_n (\alpha(G_n))^{1/n}.$$

Proof : From Theorem 3.3, we have a sequence of equilibrium strategies, $\{\hat{g}_n\}_{n \geq 1}$, that give $R(\hat{g}_n) = |\alpha(G_n)|^{1/n}$. The result follows by using Definition 2.7. ■

B. Strategic capacity

The above analysis shows that the maximum number of strings that the receiver can recover perfectly in a Stackelberg equilibrium is $\alpha(G_n)$. How large can this quantity be? And how does it scale with n ? To answer this we define the notion of a *strategic capacity* of the graph G . First, we recall a related notion, the definition of the *Shannon capacity* as given in [8].

Definition 3.1 (Shannon capacity): The Shannon capacity of the graph G is given as

$$\Theta(G) = \lim_n \alpha(G_n^{\boxtimes})^{1/n},$$

where G_n^{\boxtimes} is given by Definition 2.3.

Definition 3.2 (Strategic capacity): The strategic capacity of the graph G is given as

$$\Xi(G) = \lim_n \alpha(G_n)^{1/n},$$

where G_n is given by Definition 2.1

We now show that this limit exists. First, we state the following lemma.

Lemma 3.5 (Fekete's Lemma [9]): For a sequence $\{a_n\}_{n \geq 1}$, $a_n \in \mathbb{R}$ with $a_{m+n} \geq a_m + a_n$, the limit of the sequence $\{a_n/n\}_{n \geq 1}$ exists and is given as $\sup_n a_n/n$.

We show the following lemma which will be used to prove existence of the strategic capacity.

Lemma 3.6: Let $n \in \mathbb{N}$ and let G_n be the strategic graph. Then, for all $m, n \in \mathbb{N}$,

$$\alpha(G_{m+n}) \geq \alpha(G_m)\alpha(G_n).$$

The proof of this lemma is in the Appendix. Using this lemma we now show that the limit defined in Definition 3.2 exists.

Lemma 3.7: Let $\{G_n\}_{n \geq 1}$ be the sequence of strategic graphs. The limit given in Definition 3.2 exists.

Proof : From Lemma 3.6, we have $\alpha(G_{m+n}) \geq \alpha(G_m)\alpha(G_n)$ for all m, n . Define $\beta_n = \log(\alpha(G_n))$. Thus, we get $\beta_{m+n} \geq \beta_m + \beta_n$. Thus, from Fekete's Lemma, the limit of the sequence $\{\beta_n/n\}_{n \geq 1}$ exists and is given as $\lim_n \beta_n/n = \sup_n \beta_n/n$. From the continuity and monotonicity of $\exp(\cdot)$, we get

$$\lim_n \exp(\beta_n/n) = \sup_n \exp(\beta_n/n).$$

Substituting $\beta_n = \log(\alpha(G_n))$, we get the required result. ■

IV. THE STRATEGIC CAPACITY OF A GRAPH

In this section, we derive upper and lower bounds on the strategic capacity of the graph. First, we have the following lemma.

Lemma 4.1: Let $n \in \mathbb{N}$. Let G be the strategic graph and let G_n^{\boxtimes} be the corresponding product graph. For all x^n, y^n in G_n^{\boxtimes} such that $x^n \sim y^n$, if $u_n(x^n, x^n) = u_n(y^n, x^n)$, then $u_n(y^n, y^n) \leq u_n(x^n, y^n)$.

The proof of this lemma is in the Appendix. Using this lemma, we now show that the product graph G_n^{\boxtimes} is a subgraph of the strategic graph G_n .

Theorem 4.2: Let $n \in \mathbb{N}$. Let G_n^{\boxtimes} be a product graph and G_n be the strategic graph having a common base graph G . Then, $G_n^{\boxtimes} \subseteq G_n$.

Proof : We prove the result by induction.

Base case: For $n = 1$ both the graphs are same. Hence, the statement is trivially true.

Induction hypothesis: Assume $G_k^{\boxtimes} \subseteq G_k \quad \forall k \leq n - 1$.

Now let x^n and y^n be two vertices in G_n^{\boxtimes} where $x^n \sim y^n$. We write $x^n = (x^{n-1}, x)$, $y^n = (y^{n-1}, y)$ where $x^{n-1}, y^{n-1} \in \mathcal{X}^{n-1}$ and $x, y \in \mathcal{X}$. From the definition of G_n^{\boxtimes} , we get the following cases.

Case 1: $x^{n-1} = y^{n-1}$, $x \sim y$

In this case we have

$$u_n(x^n, x^n) - u_n(y^n, x^n) = \frac{1}{n}(u(x, x) - u(y, x)).$$

Similarly, $u_n(y^n, y^n) - u_n(x^n, y^n) = (u(y, y) - u(x, y))/n$. Since $x \sim y$, we have that either $u(x, x) \leq u(y, x)$ or $u(y, y) \leq u(x, y)$. Hence, either $u_n(x^n, x^n) < u_n(y^n, x^n)$ or $u_n(y^n, y^n) < u_n(x^n, y^n)$. Thus, $x^n \sim y^n$ in G_n .

Case 2: $x^{n-1} \sim y^{n-1}$, $x = y$

In this case we have $u_n(x^n, x^n) - u_n(y^n, x^n)$

$$= \frac{n-1}{n}(u_{n-1}(x^{n-1}, x^{n-1}) - u_{n-1}(y^{n-1}, x^{n-1}))$$

and $u_n(y^n, y^n) - u_n(x^n, y^n)$

$$= \frac{n-1}{n}(u_{n-1}(y^{n-1}, y^{n-1}) - u_{n-1}(x^{n-1}, y^{n-1})).$$

From the induction hypothesis, we have $x^{n-1} \sim y^{n-1}$ in G_{n-1} , which gives $x^n \sim y^n$ in G_n .

Case 3: $x^{n-1} \sim y^{n-1}$, $x \sim y$

Following the arguments from Case 2, we have that either $u_{n-1}(x^{n-1}, x^{n-1}) \leq u_{n-1}(y^{n-1}, x^{n-1})$ or $u_{n-1}(y^{n-1}, y^{n-1}) \leq u_{n-1}(x^{n-1}, y^{n-1})$. In this, we have the following sub-cases.

Case i: Suppose $u_{n-1}(x^{n-1}, x^{n-1}) < u_{n-1}(y^{n-1}, x^{n-1})$

Then from Assumption 2.1, we get $u_n(x^n, x^n) \leq u_n(y^n, x^n)$ and thus, $x^n \sim y^n$ in G_n .

Case ii: Suppose $u_{n-1}(x^{n-1}, x^{n-1}) = u_{n-1}(y^{n-1}, x^{n-1})$

Then, from Lemma 4.1, we have $u_{n-1}(y^{n-1}, y^{n-1}) - u_{n-1}(x^{n-1}, y^{n-1}) = 0$. Now if $u(x, x) \leq u(y, x)$ then, $u_n(x^n, x^n) \leq u_n(y^n, x^n)$. If not, then we use $u(y, y) \leq u(x, y)$ to get $u_{n-1}(y^{n-1}, y^{n-1}) \leq u_{n-1}(x^{n-1}, y^{n-1})$, thereby proving $x^n \sim y^n$ in G_n .

Case iii: Suppose $u_{n-1}(x^{n-1}, x^{n-1}) > u_{n-1}(y^{n-1}, x^{n-1})$

From Lemma 4.1 and using $x^{n-1} \sim y^{n-1}$ in G_{n-1} , we get $u_{n-1}(y^{n-1}, y^{n-1}) - u_{n-1}(x^{n-1}, y^{n-1}) < 0$ and hence $u_n(y^n, y^n) \leq u_n(x^n, y^n)$, thereby $x^n \sim y^n$ in G_n . ■

Using these results, we now present the main result.

Theorem 4.3: Let G be the strategic graph. Then

$$\alpha(G) \leq \Xi(G) \leq \Theta(G).$$

Proof : From Lemma 3.6, we have $\alpha(G_n) \geq \alpha(G)^n \quad \forall n$. Further, from Theorem 4.2, we have that $G_n^{\boxtimes} \subseteq G_n$. Thus, we get $\alpha(G_n) \leq \alpha(G_n^{\boxtimes})$ and hence

$$\alpha(G) \leq \alpha(G_n)^{1/n} \leq \alpha(G_n^{\boxtimes})^{1/n}.$$

Taking the limit, we get $\alpha(G) \leq \Xi(G) \leq \Theta(G)$. ■

The above result shows that the rate of strategic communication achievable by Stackelberg equilibrium strategies for the receiver is greater than unity for all graphs G except the complete graph. We find this to be a nontrivial conclusion.

Corollary 4.4: For any perfect graph G ,

$$\Xi(G) = \alpha(G).$$

Proof : For a perfect graph $\Theta(G) = \alpha(G)$ [8]. ■

Corollary 4.5: For a q -cycle graph where q is even, we have

$$\Xi(G) = \frac{q}{2}.$$

Proof : Cyclic graph with even number of vertices are perfect graphs. Thus, the independence number of the base graph is $\alpha(G) = q/2$. Using Corollary 4.4, we get the result. ■

Consider the following graph, in which the sender always prefers the *next* symbol over the observed symbol.







Corollary 4.6: Let q be even and consider a *shifting* sender where $u(i, i) < u(j, i)$ if and only if $j = (i + 1) \bmod q$, for all $i, j \in \mathcal{X}$. Then, we have $\Xi(G) = q/2$.

Proof : Since Assumption 2.1 holds, we have $u(i, i) > u(j, i)$ if $j \neq (i + 1) \bmod q$. Thus, $\forall i, j \in \{0, 1, \dots, q - 1\}$, $i \sim j$ if and only if $j = (i + 1) \bmod q$ and hence this graph is a q -cycle graph. Using Corollary 4.5, we get the result. ■

Since the sender is always *shifting*, it may appear that the receiver cannot recover the true signal. However, this is not the case as the induced graph is just a cycle graph.

V. EXAMPLES

Apart from the cases where the Shannon capacity is equal to the independence number of the base graph, we do not compute the strategic capacity explicitly. Determining the hardness of computing the strategic capacity remains open and is still an ongoing work. The following table mentions some of the graphs with known Shannon capacity.

Nodes	$\alpha(G)$	$\Xi(G)$	$\Theta(G)$
			
$n = 3$ 	2	2	2
	1	1	1
$n = 4$ 	2	2	2
	2	2	2
$n = 5$ 	2	$2 \leq \Xi(G) \leq \sqrt{5}$	$\sqrt{5}$

VI. CONCLUSION

We initiated a new line of inquiry in information theory by studying a strategic communication problem where the receiver aims to achieve zero-error communication with a sender who may have an incentive to misreport its signals. We formulated the problem as a game between the sender and receiver and showed that in spite of the sender being a distrustful agent, the receiver can recover an exponential number of signals. We defined a notion of strategic capacity and we proved that the strategic capacity lies between the independence number of a graph and the Shannon capacity of the graph.

APPENDIX

Proof of Lemma 3.6: Consider $\mathcal{I}_m \in \mathcal{S}(G_m)$ with $|\mathcal{I}_m| = \alpha(G_m)$ and $\mathcal{I}_n \in \mathcal{S}(G_n)$, with $|\mathcal{I}_n| = \alpha(G_n)$. Clearly, $\mathcal{I}_m \times \mathcal{I}_n \subseteq \mathcal{X}^{m+n}$. We show that $\mathcal{I}_m \times \mathcal{I}_n \in \mathcal{S}(G_{m+n})$.

Consider $x^{m+n}, y^{m+n} \in \mathcal{X}^{m+n}$ such that $x^{m+n} = (x^m, x^n)$, $y^{m+n} = (y^m, y^n)$, where $x^m, y^m \in \mathcal{I}_m$ and $x^n, y^n \in \mathcal{I}_n$. Now,

$$u_{m+n}(x^{m+n}, x^{m+n}) - u_{m+n}(y^{m+n}, x^{m+n})$$

$$= \frac{m}{m+n} (u_m(x^m, x^m) - u_m(y^m, x^m)) + \frac{n}{m+n} (u_n(x^n, x^n) - u_n(y^n, x^n)).$$

Since \mathcal{I}_m and \mathcal{I}_n are independent sets, we have $u_m(x^m, x^m) > u_m(y^m, x^m)$ and $u_n(x^n, x^n) > u_n(y^n, x^n)$. Thus, we get $u_{m+n}(x^{m+n}, x^{m+n}) > u_{m+n}(y^{m+n}, x^{m+n})$ for all $x^{m+n}, y^{m+n} \in \mathcal{I}_m \times \mathcal{I}_n, x^{m+n} \neq y^{m+n}$. Thus, $\mathcal{I}_m \times \mathcal{I}_n \in \mathcal{S}(G_{m+n})$ and $\alpha(G_{m+n}) \geq |\mathcal{I}_m| |\mathcal{I}_n| = \alpha(G_m) \alpha(G_n)$. ■

Proof of Lemma 4.1: Suppose $u_n(x^n, x^n) = u_n(y^n, x^n)$. First, we show that for all i , either $x_i = y_i$ or $x_i \sim y_i$.

Assume there exists an i such that $x_i \neq y_i$ and $x_i \not\sim y_i$. Consider the i length sequences $x^i = (x_1, \dots, x_i)$ and $y^i = (y_1, \dots, y_i)$. Since $x_i \neq y_i$ and $x_i \not\sim y_i$, from the definition of strong product, we get $x^i \not\sim y^i$. From $x^i \not\sim y^i$, we get $x^n \not\sim y^n$ where $x^n = (x^i, x_{i+1}, \dots, x_n)$ and $y^n = (y^i, y_{i+1}, \dots, y_n)$ are derived by taking the product of $G_i^{\boxtimes} \boxtimes G_{n-i}^{\boxtimes}$. However, this contradicts $x^n \sim y^n$ and hence for all i either $x_i = y_i$ or $x_i \sim y_i$. Now consider the following difference

$$u_n(x^n, x^n) - u_n(y^n, x^n) = \sum_{i: x_i \neq y_i} u(x_i, x_i) - u(y_i, x_i).$$

Since $x_i \sim y_i$ whenever $x_i \neq y_i$, we can write

$$u_n(x^n, x^n) - u_n(y^n, x^n) = (K_1 - L_1) |u(x_1, x_1) - u(y_1, x_1)|,$$

where $K_1 = |\{i : u(x_i, x_i) > u(y_i, x_i)\}|$ and $L_1 = |\{i : u(x_i, x_i) < u(y_i, x_i)\}|$. The factor $|u(x_1, x_1) - u(y_1, x_1)|$ is due to the Assumption 2.1. Similarly, we can write

$$u_n(y^n, y^n) - u_n(x^n, y^n) = (K_2 - L_2) |u(x_1, x_1) - u(y_1, x_1)|,$$

where $K_2 = |\{i : u(y_i, y_i) > u(x_i, y_i)\}|$ and $L_2 = |\{i : u(y_i, y_i) < u(x_i, y_i)\}|$. Since $x_i \sim y_i$, we have $u(y_i, y_i) < u(x_i, y_i)$ whenever $u(x_i, x_i) > u(y_i, x_i)$. Thus, we get $\{i : u(x_i, x_i) > u(y_i, x_i)\} \subseteq \{i : u(y_i, y_i) < u(x_i, y_i)\}$ and hence $K_1 \leq L_2$. Similarly, $K_2 \leq L_1$. Further, we get $K_1 = L_1$ from $u_n(x^n, x^n) = u_n(y^n, x^n)$. Thus, $K_2 - L_2 \leq L_1 - K_1 = 0$ and hence $u_n(y^n, y^n) \leq u_n(x^n, y^n)$. ■

REFERENCES

- [1] C. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.
- [2] V. P. Crawford and J. Sobel, "Strategic information transmission," *Econometrica: Journal of the Econometric Society*, pp. 1431–1451, 1982.
- [3] E. Akyol, C. Langbort, and T. Başar, "Information-theoretic approach to strategic communication as a hierarchical game," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 205–218, 2016.
- [4] E. Kamenica and M. Gentzkow, "Bayesian persuasion," *American Economic Review*, vol. 101, no. 6, pp. 2590–2615, 2011.
- [5] D. Bergemann and S. Morris, "Information design: A unified perspective," *Journal of Economic Literature*, vol. 57, no. 1, pp. 44–95, 2019.
- [6] J. Körner and A. Orlitsky, "Zero-error information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2207–2229, 1998.
- [7] S. C. Polak and A. Schrijver, "New lower bound on the Shannon capacity of c_7 from circular graphs," *Information Processing Letters*, vol. 143, pp. 37–40, 2019.
- [8] L. Lovász, "On the Shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, no. 1, pp. 1–7, 1979.
- [9] A. Schrijver, *Combinatorial optimization: polyhedra and efficiency*. Springer Science & Business Media, 2003, vol. 24.