Zero-Error Communication over Networks

Jürg Wullschleger [1]
Département d'Informatique et R. O.
Université de Montréal, Canada
e-mail: wullschj@iro.umontreal.ca

Abstract — **We introduce the *ambiguity* of a channel, which characterizes the possibility in principle of a zero-error channel to simulate any other zero-error channel. We show how to calculate the ambiguity of a virtual channel connecting two arbitrary players in a network of potential malicious players.**

I. Introduction

In [2] Shannon proposed the *zero-error capacity*, which defines the asymptotically maximal rate at which bits can be transmitted over a noisy channel without *any* error. Elias showed in [1] that channels with a zero-error capacity equal to 0 can still transmit information without any error, in the following sense: He introduced the *zero-error list-of-L capacity*—with and without feedback—, which defines the asymptotically maximal rate at which bits can be transmitted over a channel without any error, if the decoder is allowed to output a list of L strings, where one of them must be the string transmitted by the sender.

II. Zero-Error Channels

We use a definition of channels without probabilities: A $(\mathcal{X}, \mathcal{Y})$*-zero-error channel* is a relation $\mathcal{W} \subseteq \mathcal{X} \times \mathcal{Y}$, where $\mathcal{X}$ is the input domain, $\mathcal{Y}$ the output range and $\mathcal{W}$ the set of all possible input/output pairs. For every input symbol, there must exist at least one output symbol. A channel $\mathcal{W}_1$ is *achievable* by a channel $\mathcal{W}_0$ if there exists a protocol using $\mathcal{W}_0$ as communication primitive that can simulate $\mathcal{W}_1$.

A (a)-List-channel is a $(\mathcal{X}, \mathcal{Y})$-zero-error channel, with $(a)\text{-List} = \{(x, y) \in \mathcal{X} \times \mathcal{Y} | x \in y\}$, where $\mathcal{X} = \{1, \ldots, a+1\}$ and $\mathcal{Y} = \{y \subset \mathcal{X} | |y| = a\}$. (∞)-List denotes the trivial List-channel over which no communication is possible.

Theorem 1 states that every zero-error channel is equivalent to a (a)-List channel.

Theorem 1. *For every zero-error channel $\mathcal{W}$ there exists exactly one $a \in \mathbb{N} \cup \{\infty\}$ such that $\mathcal{W}$ achieves (a)-List and (a)-List achieves $\mathcal{W}$. This value a is called the* ambiguity *of $\mathcal{W}$, denoted by $A(\mathcal{W})$.*

Theorem 1 can be proven using the results of [1]. $A(\mathcal{W})$ is equal to the smallest value L for which the zero-error list-of-L capacity of $\mathcal{W}$ is non-zero. Corollary 1 shows that $A(\mathcal{W})$ characterizes the possibility of a zero-error channel $\mathcal{W}$ to simulate other zero-error channels.

Corollary 1. *For all $\mathcal{W}_1$ and $\mathcal{W}_2$, $\mathcal{W}_1$ achieves $\mathcal{W}_2$, if and only if $A(\mathcal{W}_1) \leq A(\mathcal{W}_2)$.*

While improving the efficiency of zero-error communication, feedback does not change the ambiguity of a channel, and therefore does not improve the ability of a zero-error channel to simulate other zero-error channels.

[1] Work done while at the Comp. Sci. Dept., ETH Zürich

III. Networks of Zero-Error Channels

In a network of players connected by zero-error channels, a message can either be sent directly from the sender to the receiver, or indirectly through other players. The ambiguity of a virtual channel resulting from a serial concatenation of channels is the product of their ambiguities. We call such a virtual channel malicious if it has at least one intermediate malicious player—a player that does not follow the protocol.

The communication between two arbitrary players in the network is equivalent to a parallel concatenation of all virtual channels build by serial concatenation of all channels on a path from the sender to the receiver.

We will call the set of channels which are not malicious the *honest set*. As the receiver may not know which channels belong to the honest set, we only assume that he knows that the honest set is an element of an honest set structure $\mathcal{H}$—the set of all possible honest sets.

Theorem 2 shows how the ambiguity of a parallel concatenation of channels with a given honest set structure can be calculated. Using the transformation above, it can be used to calculate the ambiguity of a virtual channel between two players in any network of potential malicious players connected by channels.

Theorem 2. *Let $W = \{\mathcal{W}_1, \ldots, \mathcal{W}_n\}$ be a set of channels and $\mathcal{H} = \{h_1, \ldots, h_k\}$ a set of honest sets. Let $\mathcal{W}_p$ be the parallel concatenation of the channels in W with the honest set structure $\mathcal{H}$. Let $S_j = \{i | j \in h_i\}$ be the set of indices of all honest sets wherein player j is. The ambiguity of $\mathcal{W}_p$ is the maximum of the sum of some integers $a_1, \ldots, a_k$,*

$$A(\mathcal{W}_p) = \max_{a_1, \ldots, a_k} \sum_{i=1}^{k} a_i$$

such that for all $j \in \{1, \ldots, n\}$

$$\sum_{i \in S_j} a_i \leq A(\mathcal{W}_j) \tag{1}$$

holds.

If we have a threshold honest set structure—if up to t channels are malicious—, then the ambiguity of the parallel concatenation can be calculated more easily. The method is given in the full version of the paper.

Acknowledgments

I thank Martin Hirt, Thomas Holenstein, Ueli Maurer and Stefan Wolf for helpful discussions.

References

[1] P. Elias, "Zero-error capacity under list decoding," *IEEE Trans. Information Theory*, vol. 34, no. 5, pp. 1070–1074, 1988.

[2] C.E. Shannon, "The zero-error capacity of a noisy channel," *IEEE Trans. Information Theory*, pp. 8–19, 1956.