On Error Correction with Feedback Under List Decoding

Ofer Shayevitz

Information Theory and Applications Center

University of California, San Diego

USA

The Liar's Game with a List

- Alice thinks of a number $m \in \{1, 2, \dots, M\}$
- Bob can ask her n binary questions (possibly adaptive)
- Alice can lie at most t times
- Bob wins the game if he can come up with a list of L numbers which includes m, otherwise loses

The Liar's Game with a List

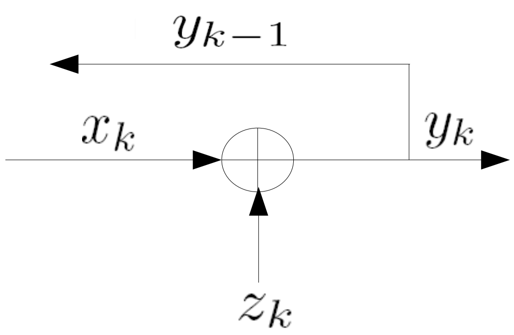
- Alice thinks of a number $m \in \{1, 2, \ldots, M\}$
- Bob can ask her n binary questions (possibly adaptive)
- Alice can lie at most t times
- Bob wins the game if he can come up with a list of L numbers which includes m, otherwise loses
- Can Bob find a strategy so that he can always win? If so, we say the game is (M, n, t, L)-winnable
- For $L = 1$, this is also known as Ulam's game
  - Solved for small t, or any t and large enough n
  - Notoriously difficult in general

Error Correction with Feedback

- Game equivalent to error correction with feedback and list-of-L decoding:

$$m \in \{1, \ldots, M\}$$

$$\sum_{k=1}^{n} z_k \le t$$



$$m \in \Delta(y^n)$$

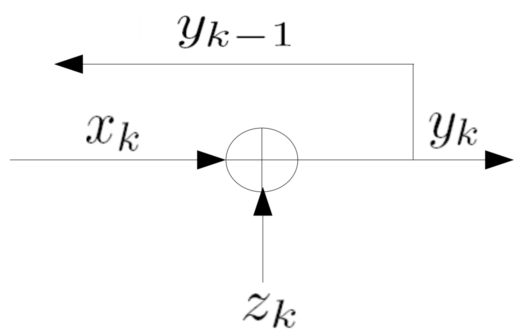
$$|\Delta(y^n)| \le L$$

Error Correction with Feedback

- Game equivalent to error correction with feedback and list-of-L decoding:

$$m \in \{1, \ldots, M\}$$

$$\sum_{k=1}^{n} z_k \leq t$$



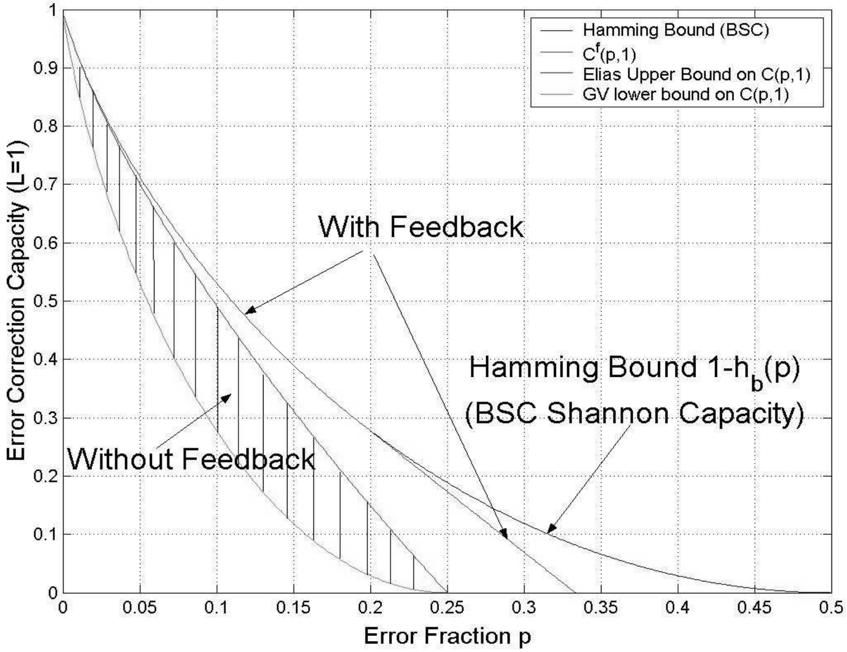
$$m \in \Delta(y^n)$$

$$|\Delta(y^n)| \leq L$$

- We consider the asymptotic case:
  - Set $t = np$ for some $0 < p < 1$
  - Rate R is *achievable* if the game is $(2^{nR}, n, np, L)$-winnable $\forall$ large n
  - Let $C^f(p, L)$ be the supremum over all achievable rates, namely the *error correction capacity with feedback and a list-of-L decoding*
  - Let $C(p, L)$ be the corresponding quantity in the absence of feedback (non-adaptive questions)

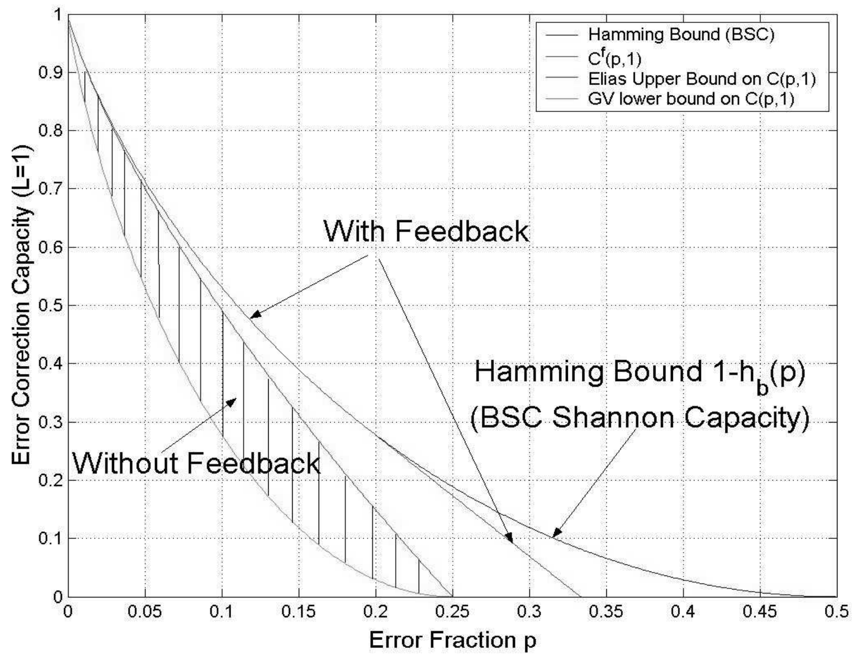
Known Results and Motivation

- For $L = 1$, only bounds for $C(p, 1)$ are known.
- In contrast, $C^f(p, 1)$ is known exactly [*Berlekamp'64*] [*Zigangirov'76*]
- $1 - h_b(p) - \frac{1}{L} \le C(p, L) \le 1 - h_b(\lambda_{p,L})$ for some $\lambda_{p,L} > p$ [*Blinovsky'86*] [*Elias'91*] [Guruswami'01]



Known Results and Motivation

- For $L = 1$, only bounds for $C(p, 1)$ are known.
- In contrast, $C^f(p, 1)$ is known exactly [*Berlekamp'64*] [*Zigangirov'76*]
- $1 - h_b(p) - \frac{1}{L} \leq C(p, L) \leq 1 - h_b(\lambda_{p,L})$ for some $\lambda_{p,L} > p$ [*Blinovsky'86*] [*Elias'91*] [Guruswami'01]



- What can we say about $C^f(p, L)$?

State Space Formulation [Berlekamp'64]

- Bob's question is a partition $A \cup \bar{A} = \{1, \dots, M\}$?
- Alice's answer *votes against* either A or $\bar{A}$
- Bob keeps count of the votes against each $m \in \{1, \dots, M\}$
- Bob wins iff after n rounds, there are no more than L messages that accumulated t votes or less

State Space Formulation *[Berlekamp'64]*

- Bob's question is a partition $A \cup \bar{A} = \{1, \ldots, M\}$?
- Alice's answer *votes against* either A or $\bar{A}$
- Bob keeps count of the votes against each $m \in \{1, \ldots, M\}$
- Bob wins iff after n rounds, there are no more than L messages that accumulated t votes or less
- The *state of the game* is $\boldsymbol{s} = (s_0, s_1, \ldots, s_t)$, where s_i is the number of messages that accumulated $t - i$ votes
  - $\boldsymbol{s}$ is called an n-state, if there are n questions still remaining
  - The game initializes in the state $\boldsymbol{I}_M^t = (0, 0, \ldots, 0, M)$.
  - Bob wins iff the game ends in a 0-state $\boldsymbol{s}$ such that $\sum s_i \leq L$
  - Such a state is called a L*-winning* 0*-state*

State Space Formulation - cont.

- A question induces a partition of the current state $\boldsymbol{s} = \boldsymbol{a} + \bar{\boldsymbol{a}}$
- The answer *reduces* the state into either of the states

$$\boldsymbol{x} = T\boldsymbol{a} + \bar{\boldsymbol{a}} \qquad \boldsymbol{y} = \boldsymbol{a} + T\bar{\boldsymbol{a}}$$

where the *translation operator* T is defined by

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_t)\,, \quad T\boldsymbol{a} = (a_1, a_2, \ldots, a_t, 0)$$

- We (recursively) define a state to be a L*-winning* n*-state*, if it can be reduced into two L-winning $(n-1)$-states
- The game is (M, n, t, L)-winnable iff $\boldsymbol{I}_M^t = (0, 0, \ldots, 0, M)$ is a L-winning n-state.

Conservation of Volume

- Define the *Volume* of an n-state:

$$V_n(\boldsymbol{s}) \triangleq \sum_{k=0}^{t} s_k \sum_{j=0}^{k} \binom{n}{j}$$

  - Accumulated volume of spheres around each message, radius equals the corresponding number of remaining votes
  - $V_0(\boldsymbol{s}) = \sum s_i$
  - $V_n(\boldsymbol{I}_M^t) = M \cdot \sum_{j=0}^{t} \binom{n}{j}$

Conservation of Volume

- Define the *Volume* of an n-state:

$$V_n(\boldsymbol{s}) \triangleq \sum_{k=0}^{t} s_k \sum_{j=0}^{k} \binom{n}{j}$$

  - Accumulated volume of spheres around each message, radius equals the corresponding number of remaining votes
  - $V_0(\boldsymbol{s}) = \sum s_i$
  - $V_n(\boldsymbol{I}_M^t) = M \cdot \sum_{j=0}^{t} \binom{n}{j}$

Lemma [*Berlekamp'64*] : If the n-state $\boldsymbol{s}$ can be reduced to $\boldsymbol{x}, \boldsymbol{y}$ then

$$V_n(\boldsymbol{s}) = V_{n-1}(\boldsymbol{x}) + V_{n-1}(\boldsymbol{y})$$

The Generalized Volume Bound (GVB)

Theorem: If $\boldsymbol{s}$ is an L-winning n-state, then

$$V_n(\boldsymbol{s}) \leq L \cdot 2^n$$

The Generalized Volume Bound (GVB)

Theorem: If $\boldsymbol{s}$ is an L-winning n-state, then

$$V_n(\boldsymbol{s}) \leq L \cdot 2^n$$

- *Proof:* (trivial generalization of [*Berlekamp '64*])
  - Suppose $\boldsymbol{s}$ is reduced to $\boldsymbol{x}, \boldsymbol{y}$
  - By conservation of volume and wlog, $V_{n-1}(\boldsymbol{x}) \geq \frac{1}{2} V_n(\boldsymbol{s})$
  - Worst case – volume reduced by a factor of at most 2 each round
  - A L-winning 0-state must satisfy $V_0(\boldsymbol{s}) = \sum s_i \leq L$
- A necessary condition for R to be achievable is

$$V_n(\boldsymbol{I}^{np}_{2^{nR}}) = 2^{nR} \cdot \sum_{j=0}^{np} \binom{n}{j} \leq L \cdot 2^n$$

- Hence $R \leq 1 - h_b(p)$ (not surprisingly..)

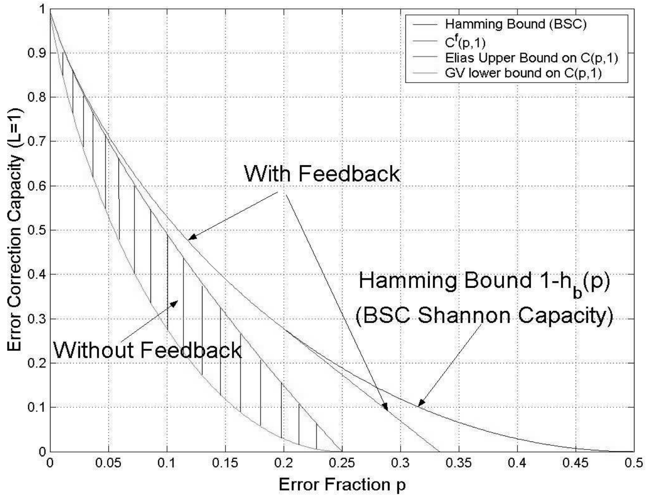
The Translation Property (TP) for $L = 1$

Theorem [*Berlekamp'64*] : If $\boldsymbol{s}$ is an 1-winning n-state and $\sum s_i \geq 3$, then $T\boldsymbol{s}$ is a 1-winning $(n-3)$-state

The Translation Property (TP) for $L = 1$

Theorem [*Berlekamp'64*] : If $\boldsymbol{s}$ is an 1-winning n-state and $\sum s_i \geq 3$, then $T\boldsymbol{s}$ is a 1-winning $(n-3)$-state

- If the number of permitted lies is reduced by one, the number of questions to win is reduced by at least 3.
- In conjunction with the GVB, gives the linear (tangential) part of the capacity curve
- Can we generalize the TP to $L > 1$?
- Well, almost..



Restricting the Family of States/Strategies

- Let Λ_L to be the set of all states $\boldsymbol{s}$ such that either
  - $\boldsymbol{s} = (s_0, s_1, \ldots, L + j, 0^k, L, 0, \ldots, 0)$ for some $j, k \geq 0$
  - $\boldsymbol{s} = (s_0, s_1, \ldots, 2L + j, 0, \ldots, 0)$ for some $k \geq 0$
  - $\sum s_i \leq 2L$

Restricting the Family of States/Strategies

- Let Λ_L to be the set of all states $\boldsymbol{s}$ such that either
  - $\boldsymbol{s} = (s_0, s_1, \ldots, L + j, 0^k, L, 0, \ldots, 0)$ for some $j, k \geq 0$
  - $\boldsymbol{s} = (s_0, s_1, \ldots, 2L + j, 0, \ldots, 0)$ for some $k \geq 0$
  - $\sum s_i \leq 2L$
- Note that for $L = 1$, Λ_1 is the set of all states
- We recursively define a state $\boldsymbol{s} \in \Lambda_L$ to be a Λ_L-winning n-state, if it can be reduced to two Λ_L-winning $(n-1)$-states.
- $C^f_\Lambda(p, L)$ is the error correction capacity w.r.t. Λ_L under a list-of-L decoding
- $C^f_\Lambda(p, L) \leq C^f(p, L)$

The Integer Sequence π_L

- Let π_L be the minimal positive integer so that the state

$$\boldsymbol{s} = (0^{\pi_L - 1}, L, L+1)$$

is a L-loosing $(2\pi_L + 1)$-state.

The Integer Sequence π_L

- Let π_L be the minimal positive integer so that the state

$$\boldsymbol{s} = (0^{\pi_L - 1}, L, L+1)$$

is a L-loosing $(2\pi_L + 1)$-state.

  - For $L = 1$ we have $V_3((1,2)) = 9 > 2^3$, hence $(1,2)$ is a 1-losing 3-state, and so $\pi_1 = 1$.
  - For $L > 1$, by exhaustive search.. $\{\pi_L\}_{L=1}^{\infty} = \{1, 2, 4, 7, \ldots\}$

The Integer Sequence π_L

- Let π_L be the minimal positive integer so that the state

$$\boldsymbol{s} = (0^{\pi_L - 1}, L, L+1)$$

  is a L-loosing $(2\pi_L + 1)$-state.
  - For $L = 1$ we have $V_3((1,2)) = 9 > 2^3$, hence $(1,2)$ is a 1-losing 3-state, and so $\pi_1 = 1$.
  - For $L > 1$, by exhaustive search.. $\{\pi_L\}_{L=1}^{\infty} = \{1, 2, 4, 7, \ldots\}$
- Using the GVB we can show that

$$\pi_L \leq \mu_L = \inf\left\{\mu \in \mathbb{N} \,:\, 2^{2\mu} > L\binom{2\mu+1}{\mu}\right\} = O(L^2)$$

- However $\{\mu_L\}_{L=1}^{\infty} = \{1, 4, 11, 20, \ldots\}$, seems far from tight.

The Generalized Translation Property (GTP)

Theorem: If $\boldsymbol{s}$ is a Λ_L-winning n-state and

$$\sum_{i=\pi_L-1}^{t} s_i \geq 2L + 1$$

then $T^{\pi_L}\boldsymbol{s}$ is a Λ_L-winning $(n - (2\pi_L + 1))$-state.

The Generalized Translation Property (GTP)

Theorem: If $\boldsymbol{s}$ is a Λ_L-winning n-state and

$$\sum_{i=\pi_L-1}^{t} s_i \geq 2L+1$$

then $T^{\pi_L}\boldsymbol{s}$ is a Λ_L-winning $(n-(2\pi_L+1))$-state.

- If the number of permitted lies is reduced by π_L, the number of questions to win is reduced by at least $2\pi_L+1$.
- For $L=1$, we get the original TP
- Combining the GTP and the GVB, we derive an upper bound on $C_\Lambda^f(p,L)$

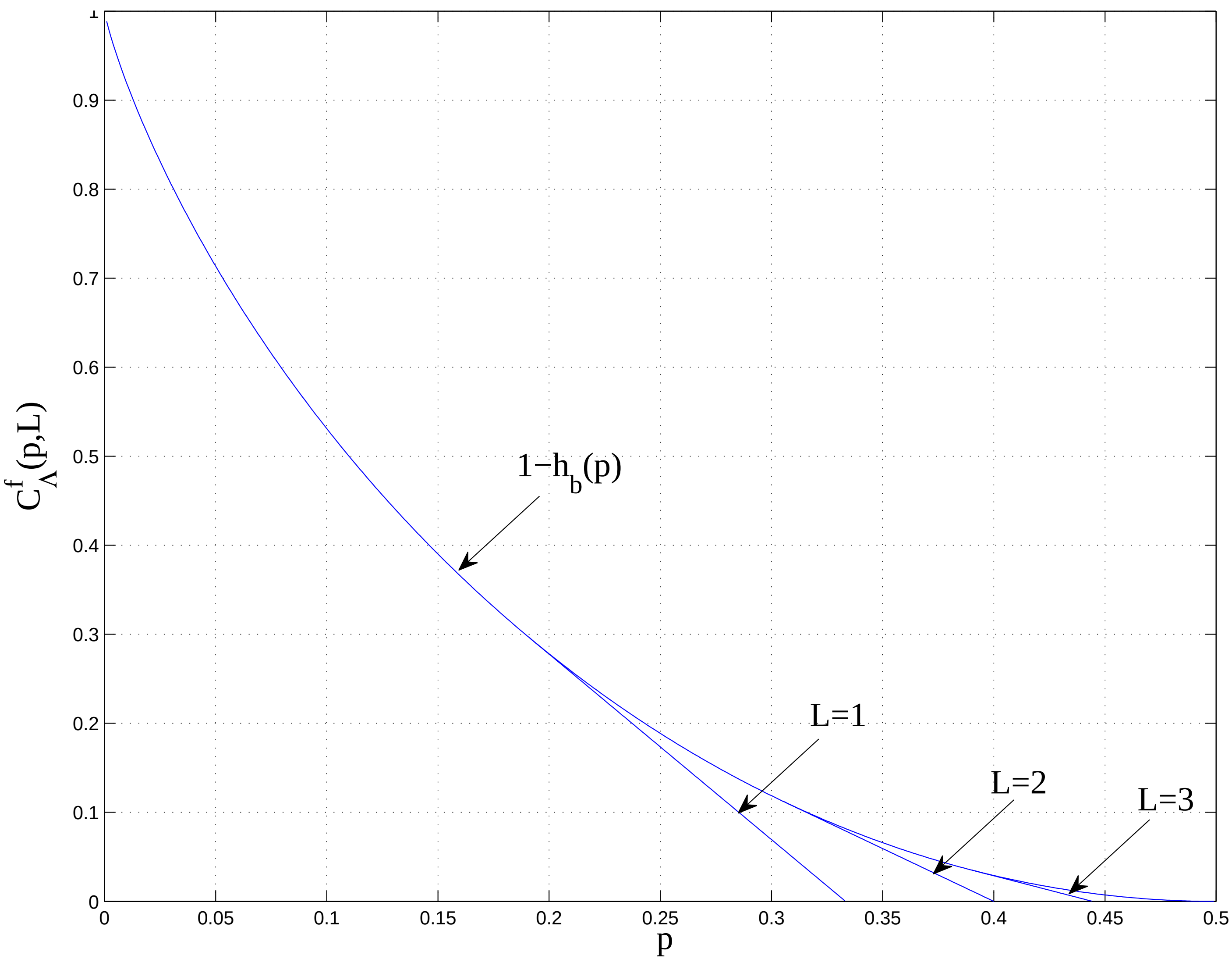
An Upper Bound on $C_\Lambda^f(p, L)$

Theorem: The following upper bound holds

$$C_\Lambda^f(p,L) \le \begin{cases} 1 - h_b(p) & 0 \le p \le p_L \\ a_L\left(1 - \frac{2\pi_L+1}{\pi_L}p\right) & p_L \le p \le \frac{\pi_L}{2\pi_L+1} \\ 0 & p \ge \frac{\pi_L}{2\pi_L+1} \end{cases}$$

where a_L, p_L are such that the straight line part is tangent to $1 - h_b(p)$ at p_L.

An Upper Bound on $C_{\Lambda}^{f}(p, L)$



Concluding Remarks

- Upper bound on achievable rates for a large family of strategies were derived
- However, possibly some loss incurred by the Λ_L constraint
- Some hope yet – The constraint seems weak since the partition of the $2L$ bottom messages seems important only near the end of the game
- Can we prove that for any L-winning n-state there exists a dominating Λ_L-winning $(n + o(n))$-state?
- An affirmative answer will result in $C^f_\Lambda(p, L) = C^f(p, L)$
- For $L = 1$ achievability was proved constructively, sometimes via very simple schemes [Schalkwijk'71] [Zigangirov'76] [Ahlswede et al'06]. Can we do the same for $L > 1$?