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 $m \in \{1, 2, \ldots, M\}$
- 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
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
Game equivalent to error correction with feedback and list-of-$L$ decoding:

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

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

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

$$|\Delta(y^n)| \leq L$$
Game equivalent to error correction with feedback and list-of-$L$ decoding:

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

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

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]

- $1 - h_b(p) - \frac{1}{L} \leq C(p, L) \leq 1 - h_b(\lambda_{p,L})$ 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]

$$1 - h_b(p) - \frac{1}{L} \leq C(p, L) \leq 1 - h_b(\lambda_{p,L}) \text{ for some } \lambda_{p,L} > p$$

[Blinovsky’86] [Elias’91] [Guruswami’01]

- What can we say about $C^f(p, L)$?
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
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 $s = (s_0, s_1, \ldots, s_t)$, where $s_i$ is the number of messages that accumulated $t - i$ votes

$s$ is called an $n$-state, if there are $n$ questions still remaining

The game initializes in the state $I^t_M = (0, 0, \ldots, 0, M)$.

Bob wins iff the game ends in a 0-state $s$ such that $\sum s_i \leq L$

Such a state is called a $L$-winning 0-state
A question induces a partition of the current state \( s = a + \bar{a} \)

The answer reduces the state into either of the states

\[
x = Ta + \bar{a} \quad \text{and} \quad y = a + T\bar{a}
\]

where the translation operator \( T \) is defined by

\[a = (a_0, a_1, \ldots, a_t), \quad Ta = (a_1, a_2, \ldots, a_t, 0)\]

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 \( I_M^t = (0, 0, \ldots, 0, M) \) is a \( L \)-winning \( n \)-state.
Define the *Volume* of an $n$-state:

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

Accumulated volume of spheres around each message, radius equals the corresponding number of remaining votes

- $V_0(s) = \sum s_i$
- $V_n(I_M^t) = M \cdot \sum_{j=0}^{t} \binom{n}{j}$
Conservation of Volume

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

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

Accumulated volume of spheres around each message, radius equals the corresponding number of remaining votes:

- $V_0(s) = \sum s_i$
- $V_n(I^t_M) = M \cdot \sum_{j=0}^{t} \binom{n}{j}$

**Lemma [Berlekamp’64]**: If the $n$-state $s$ can be reduced to $x, y$ then

$$V_n(s) = V_{n-1}(x) + V_{n-1}(y)$$
Theorem: If $s$ is an $L$-winning $n$-state, then

$$V_n(s) \leq L \cdot 2^n$$
The Generalized Volume Bound (GVB)

**Theorem:** If $s$ is an $L$-winning $n$-state, then

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

**Proof:** (trivial generalization of [Berlekamp ’64])

- Suppose $s$ is reduced to $x, y$
- By conservation of volume and wlog, $V_{n-1}(x) \geq \frac{1}{2}V_n(s)$
- Worst case – volume reduced by a factor of at most $2$ each round
- A $L$-winning 0-state must satisfy $V_0(s) = \sum s_i \leq L$

A necessary condition for $R$ to be achievable is

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

Hence $R \leq 1 - h_b(p)$ (not surprisingly..)
**The Translation Property (TP) for** $L = 1$

**Theorem** [Berlekamp’64]: If $s$ is an $1$-winning $n$-state and $\sum s_i \geq 3$, then $Ts$ is a $1$-winning $(n - 3)$-state.
The Translation Property (TP) for $L = 1$

**Theorem** [Berlekamp’64]: If $s$ is an 1-winning $n$-state and $\sum s_i \geq 3$, then $Ts$ 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..
Let $\Lambda_L$ to be the set of all states $s$ such that either

1. $s = (s_0, s_1, \ldots, L + j, 0^k, L, 0, \ldots, 0)$ for some $j, k \geq 0$
2. $s = (s_0, s_1, \ldots, 2L + j, 0, \ldots, 0)$ for some $k \geq 0$
3. $\sum s_i \leq 2L$
Restricting the Family of States/Strategies

Let $\Lambda_L$ to be the set of all states $s$ such that either

- $s = (s_0, s_1, \ldots, L + j, 0^k, L, 0, \ldots, 0)$ for some $j, k \geq 0$
- $s = (s_0, s_1, \ldots, 2L + j, 0, \ldots, 0)$ for some $k \geq 0$
- $\sum s_i \leq 2L$

Note that for $L = 1$, $\Lambda_1$ is the set of all states

We recursively define a state $s \in \Lambda_L$ to be a $\Lambda_L$-winning $n$-state, if it can be reduced to two $\Lambda_L$-winning $(n - 1)$-states.

$C^f_\Lambda(p, L)$ is the error correction capacity w.r.t. $\Lambda_L$ under a list-of-$L$ decoding

$C^f_\Lambda(p, L) \leq C^f(p, L)$
Let $\pi_L$ be the minimal positive integer so that the state

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

is a $L$-loosing $(2\pi_L + 1)$-state.
Let $\pi_L$ be the minimal positive integer so that the state
\[ s = (0^{\pi_L-1}, L, L+1) \]
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.. $\{\pi_L\}_{L=1}^{\infty} = \{1, 2, 4, 7, \ldots\}$
Let $\pi_L$ be the minimal positive integer so that the state

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

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 \( s \) is a \( \Lambda_L \)-winning \( n \)-state and

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

then \( T^{\pi_L} s \) is a \( \Lambda_L \)-winning \( (n - (2\pi_L + 1)) \)-state.
The Generalized Translation Property (GTP)

Theorem: If \( s \) is a \( \Lambda_L \)-winning \( n \)-state and

\[
\sum_{i=\pi L - 1}^{t} s_i \geq 2L + 1
\]

then \( T^{\pi L} s \) is a \( \Lambda_L \)-winning \( (n - (2\pi L + 1)) \)-state.

- If the number of permitted lies is reduced by \( \pi_L \), 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 \( C^f_\Lambda(p, L) \).
Theorem: The following upper bound holds

\[ C_{\Lambda}^f(p, L) \leq \begin{cases} 
1 - h_b(p) & 0 \leq p \leq p_L \\
 a_L \left(1 - \frac{2\pi L + 1}{\pi L} p\right) & p_L \leq p \leq \frac{\pi L}{2\pi L + 1} \\
0 & p \geq \frac{\pi L}{2\pi L + 1} 
\end{cases} \]

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 $C^f_{\Lambda}(p, L)$
Concluding Remarks

- Upper bound on achievable rates for a large family of strategies were derived
- However, possibly some loss incurred by the $\Lambda_L$ 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 $\Lambda_L$-winning $(n + o(n))$-state?
- An affirmative answer will result in $C^f_{\Lambda}(p, L) = C^f_{\Lambda}(p, L)$
- 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 $L > 1$?