On Error Correction with Feedback under List Decoding

Ofer Shayevitz
Information Theory and Applications Center
University of California, San Diego
La Jolla, CA 92093
ofersha@ucsd.edu

***Abstract*— This work provides some preliminary results on the problem of error correction in the presence of noiseless feedback, where list-of-L decoding is allowed. The methods introduced by Berlekamp for the list-of-1 setting are generalized, and some basic finite-block constraints are described. These constraints are then combined to derive an upper bound on the asymptotically achievable rates for a large family of strategies, as a function of the maximal error fraction p and the list size L.**

I. Introduction

Consider the following game played by Alice and Bob. Alice picks one of M possible objects, and Bob is allowed to ask n yes/no questions, trying to determine which object was selected. If Alice is always truthful, then $n = \lceil \log M \rceil$ questions are obviously both necessary and sufficient to that end[1]. Now, suppose Alice is allowed to *lie* up to t times. How many questions $n(M,t)$ does Bob need now? Alternatively, given n questions, what is the maximal number of objects $M(n,t)$ that Bob can separate? This version of the "twenty questions game" with lies is known as *Ulam's game* [14].

Ulam's game can be equivalently viewed as a problem of error-free communication between a transmitter and a receiver, taking place over a binary channel with noiseless feedback. The objects are now called messages, the yes/no questions are transmitted bits, the answers are received bits, and the lies are now errors introduced by the channel (we will find it convenient to use these terms interchangeably). Since in Ulam's game the lies are due to Alice, the noiseless feedback link is required to guarantee that errors are causally known at the transmitter, making the equivalence complete. Any (M,n,t) winning strategy for Ulam's game is therefore equivalent to a feedback transmission scheme or an "error-correcting code with feedback", which has M messages and can correct up to t errors over a fixed block length of n channel uses.

Ulam's game was originally analyzed in a seminal work by Berlekamp [2], in the context of error correction. In that work, an elegant state-space formulation of the game was provided, and some fundamental constraints on the structure of winning states were derived, in the form of the *volume bound* and the *translation property*. Berlekamp's techniques and results were extensively used by others to analyze and provide partial solutions to Ulam's game with a fixed number of lies [11][13][4][5]. In a communication setting however, a more reasonable and acceptable model is one where the number of errors scales linearly with the block length, i.e., $t = \lceil np \rceil$ for some $p \in (0,1)$, and the figure of merit is the *rate* $\frac{1}{n}\log M$. In his work [2], Berlekamp also provided an upper bound on asymptotically achievable rates as a function of the maximal error fraction p. For small p, this bound is simply the *Hamming bound* $1-h_b(p)$, where $h_b(\cdot)$ is the binary entropy function. For large p, the bound continues tangent to the Hamming bound, intersecting the p-axis at $p = \frac{1}{3}$. The straight line part of the bound was shown to be tight, and later so was the convex part [15].

In contrast to this sharp result, only upper and lower bounds on the asymptotically achievable rates of (one-way) binary $\lceil np \rceil$-error-correcting block codes are known [10]. The upper bounds are strictly below the rates achievable using feedback for any $0 < p < \frac{1}{3}$; in fact, without feedback no positive rate can be asymptotically attained for $p > \frac{1}{4}$. Thus, feedback increases the set of achievable rates when all error patterns up to fraction p must be corrected. This is in contrast to the case of the binary symmetric channel (BSC) with crossover probability p, where the random error patterns are to be corrected with high probability, and feedback does not increase the Shannon capacity [12].

In an effort to better understand the gap between the Shannon capacity of the BSC and the upper bounds on achievable rates for error correction without feedback, Elias [7] introduced the relaxed notion of *list decoding*, where decoding is declared successful if and only if the receiver can provide a list of $L > 1$ messages which includes the true message. As it turns out, the achievable rates for error correction under list decoding can be made arbitrarily close to the Hamming bound (and hence to the capacity of the BSC) for a large enough but fixed list size L. The concept of list decoding has been proved very useful for understanding the structure of the Hamming space, and to have many applications within and outside coding theory, see [8] and references therein.

Motivated by the discussion above, we turn to consider the problem of list decoding for error correction in the presence of noiseless feedback. We generalize Berlekamp's volume bound and translation property, providing basic constraints on the structure of winning states in this setting. However, as opposed

[1] All logarithms in this paper are taken to the base of 2.

to the list-of-1 case, our generalized translation property is shown to hold for a large family of game strategies, but not for all. We then proceed and use these constraints to derive a preliminary asymptotic result – an upper bound on achievable rates for error correction as a function of the maximal error fraction p and the list size L, under the considered family of strategies. Some speculations on the applicability of our bound in the general case are shortly discussed.

II. Problem Formulation

In this section, we introduce a state-space formulation of Ulam's game, mostly following [2][6]. Let $\mathcal{X} = \{1, 2, \ldots, M\}$ be the message set. A general binary question is a function $F : \mathcal{X} \mapsto \{0, 1\}$, where $F(x)$ is the true answer corresponding to the message $x \in \mathcal{X}$. Any question induces a binary partition of the message set into $\mathcal{X} = F^{-1}(0) \cup F^{-1}(1)$. If the (not necessarily true) answer to a question F is $b \in \{0, 1\}$, then we say that the answer *votes against* each message in $F^{-1}(1-b)$.

A vector $\boldsymbol{s} = (s_0, s_1, \ldots, s_t) \in \mathbb{N}^{t+1}$ such that

$$s^{(0)} \triangleq \sum_{k=0}^{t} s_k \leq M$$

is called a *state vector* for a game with M messages and t errors, where s_k represents the number of messages that accumulated exactly $t - k$ votes. Since at any point during the game the true message accumulates no more than t votes against it, messages that accumulated more than t votes do not affect the state of the game. The state $\boldsymbol{s}$ is said to be a *n-state* if it is a state vector of a game with n questions remaining.

Define the *translation operator* T over state vectors:

$$T\boldsymbol{s} = (s_1, s_2, \ldots, s_t, 0)$$

and let T^k be its k-fold iteration. A pair of vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^{t+1}$ such that $\boldsymbol{s} = \boldsymbol{a}+\boldsymbol{b}$ are said to be a *partition* of the state vector $\boldsymbol{s}$. It is easy to see that the partition of the message set induced by a question F corresponds to a unique partition of the state vector. Thus, an answer to the question F *reduces* the state vector $\boldsymbol{s}$ into either of the states

$$T\boldsymbol{a} + \boldsymbol{b}\,, \quad \boldsymbol{a} + T\boldsymbol{b} \tag{1}$$

In a list-of-L setting, the game is won if and only if no more than L messages accumulated less than $t + 1$ votes when the game ends. In state-space formulation this means that the 0-state $\boldsymbol{s}$ satisfies $s^{(0)} \leq L$, in which case the state is called a *L-winning 0-state*. A state $\boldsymbol{s}$ is (recursively) defined to be a *L-winning n-state* if there exists a partition $\boldsymbol{a}, \boldsymbol{b}$ (i.e., a question F) such that $\boldsymbol{s}$ can be reduced (in the sense of (1)) into two L-winning $(n-1)$-states. Such a state $\boldsymbol{s}$ is further called a *borderline* L-winning n-state, if it is not L-winning $(n-1)$-state. Clearly, a list-of-L Ulam's game with M messages and t errors can be won in n steps if and only if the $t+1$-dimensional initial state vector $\boldsymbol{I}^t_M \triangleq (0, 0, \ldots, 0, M)$ is a L-winning n-state.

Returning to the asymptotic setting of error-correction with feedback, we say that a rate R is *(p, L)-achievable* (or simply *achievable*) if for all n large enough, $\boldsymbol{I}^{\lceil np \rceil}_{\lceil 2^{nR} \rceil}$ is a L-winning n-state. The *list-of-L error-correction capacity with feedback* is thus defined to be supremum over all (p, L)-achievable rates, and is denoted by $C^f(p, L)$.

III. Properties of Winning States

A state $\boldsymbol{s}$ is said to *dominate* another state $\boldsymbol{t}$, if

$$s^{(k)} \geq t^{(k)}$$

for any $k \geq 0$, where

$$s^{(k)} \triangleq \sum_{j=k}^{t} s_j$$

Lemma 1: If $\boldsymbol{s}$ dominates $\boldsymbol{t}$ and $\boldsymbol{s}$ is a L-winning n-state, then $\boldsymbol{t}$ is a L-winning n-state.

Proof: Loosely speaking, it can be shown that $\boldsymbol{s}$ can be transformed into $\boldsymbol{t}$ by left-shifting some elements, and then possibly erasing some elements. It is easy to verify that this implies the winning strategy for $\boldsymbol{s}$ induces a winning strategy for $\boldsymbol{t}$. We omit the formal proof of this intuitive result, see [6] for the case of $L = 1$. ■

An important characteristic of a n-state is its *volume*, which is the accumulated volume of Hamming spheres placed around each message, with a radius equal to the number of votes remaining for the message to remain in the game [2], i.e.,

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

The next basic result is from [2], the proof is reproduced here for completeness.

Lemma 2 (Conservation of Volume [2]): Let $\boldsymbol{s}$ be any n-state and $\boldsymbol{a}, \boldsymbol{b}$ any corresponding partition. Then,

$$V_n(\boldsymbol{s}) = V_{n-1}(T\boldsymbol{a} + \boldsymbol{b}) + V_{n-1}(\boldsymbol{a} + T\boldsymbol{b}) \tag{2}$$

Proof: The factorial identity $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ implies that $V_n(\boldsymbol{s}) = V_{n-1}(\boldsymbol{s}) + V_{n-1}(T\boldsymbol{s})$. Therefore,

$$\begin{aligned} V_n(\boldsymbol{s}) &= V_n(\boldsymbol{a}) + V_n(\boldsymbol{b}) \\ &= V_{n-1}(\boldsymbol{a}) + V_{n-1}(T\boldsymbol{a}) + V_{n-1}(\boldsymbol{b}) + V_{n-1}(T\boldsymbol{b}) \\ &= V_{n-1}(T\boldsymbol{a} + \boldsymbol{b}) + V_{n-1}(\boldsymbol{a} + T\boldsymbol{b}) \end{aligned}$$

■

The following Theorem characterizes L-winning n-states in terms of their volume. It is a direct consequence of Lemma 2, and a trivial generalization of the 1-winning n-state result from [2].

Theorem 1 (Generalized Volume Bound): Suppose $\boldsymbol{s}$ is a L-winning n-state. Then

$$V_n(\boldsymbol{s}) \leq L \cdot 2^n \tag{3}$$

Proof: The proof is by induction, differing from [2] only in the induction basis. For $n = 0$, a L-winning 0-state $\boldsymbol{s}$ must satisfy $\boldsymbol{s}^{(0)} \leq L$, and so the volume bound trivially holds. Now assume the bound holds for $n - 1$. Since $\boldsymbol{s}$ is a L-winning n-state, there must exist a partition $\boldsymbol{a}, \boldsymbol{b}$ so that both $T\boldsymbol{a} +$

$\boldsymbol{b}, \boldsymbol{a}+T\boldsymbol{b}$ are L-winning $(n-1)$-states. Using Lemma 2 and the induction hypothesis we get

$$V_n(\boldsymbol{s}) = V_{n-1}(T\boldsymbol{a}+\boldsymbol{b}) + V_{n-1}(\boldsymbol{a}+T\boldsymbol{b}) \le L \cdot 2^n \quad (4)$$

■

The following Theorem has been proved by Berlekamp for a list-of-1, and then used to provide the linear part of the error-correction capacity bound.

Theorem 2 (Translation Property [2]): If $\boldsymbol{s}$ is a 1-winning n-state with $s^{(0)} \ge 3$, then $T\boldsymbol{s}$ is a 1-winning $(n-3)$-state.

We would like to generalize the translation property for the case of $L > 1$. However, it turns out that in order to obtain such a generalization we need to limit the family of allowable game strategies. This is of course unfortunate, since the corresponding asymptotical bound we later derive applies only to such strategies. Nevertheless, this class of strategies is large and there is some reason to speculate that asymptotically it may be sufficient to consider. This point is shortly discussed in Section V.

Lemma 3: Define the state $\boldsymbol{t}_{j,k,L} = (0^j, L) + (0^k, L)$. Then $\boldsymbol{t}_{L,j,k}$ is a borderline L-winning $(j+k+1)$-state, and satisfies the corresponding generalized volume bound with equality.

Proof: Consider the game strategy where the upper L objects are always played against the lower L objects. It is easy to verify that in the worst case, Alice would always vote against the lower L objects, in which case Bob wins the game after having asked exactly $j+k+1$ question. Without loss of generality assume that $j \le k$, and so the corresponding volume is given by

$$\begin{aligned} & V_{j+k+1}(\boldsymbol{t}_{j,k,L}) = \\ & = 2L \sum_{m=0}^{j} \binom{j+k+1}{m} + L \sum_{m=j+1}^{k} \binom{j+k+1}{m} \\ & = L \sum_{m=0}^{j+k+1} \binom{j+k+1}{m} = L \cdot 2^{j+k+1} \end{aligned}$$

and it is easily verified that

$$V_{j+k}(\boldsymbol{t}_{j,k,L}) > L \cdot 2^{j+k}$$

completing the proof. ■

Let $B_L\boldsymbol{s}$ be the state obtained from $\boldsymbol{s}$ by erasing all but the bottom $2L$ objects[2]. Now, define Λ_L to be the set of all states $\boldsymbol{s}$ such that either $B^L\boldsymbol{s} = \boldsymbol{t}_{j,k,L}$ for some $j,k \ge 0$, or $s^{(0)} < 2L$. Note that for $L=1$ the constraints are trivially satisfied so Λ_1 includes all possible state vectors; this however does not hold for $L>1$. We now define the notion of winning with respect to Λ_L. Any L-winning 0-state is also called a *Λ_L-winning 0-state*. A state $\boldsymbol{s}$ is (recursively) defined to be a *Λ_L-winning n-state*, if $\boldsymbol{s} \in \Lambda_L$ and can be reduced into two Λ_L-winning $(n-1)$-states. Thus, winning with respect to Λ_L constrains the allowable question strategies roughly to those that maintain the last $2L$ objects to be in a $\boldsymbol{t}_{j,k,L}$-type state. This constraint can in fact be significantly relaxed without essentially changing the results, but this step is avoided for simplicity of exposition. Obviously, any Λ_L-winning n-state is also a L-winning n-state, but not necessary vice versa. In the asymptotical regime, one can correspondingly define the notion of an error-correction capacity $C^f_\Lambda(p,L)$ with respect to Λ_L as the supremum over all (p,Λ_L)-achievable rates R,[3] i.e., when strategies are limited to produce only states within Λ_L. Of course, $C^f_\Lambda(p,L) \le C^f(p,L)$.

Another definition is required before we can proceed to generalize the translation property. Define π_L to be the minimal positive integer so that the state $(0^{\pi_L-1}, L, L+1)$ is a L-loosing $(2\pi_L+1)$-state. For $L=1$, $V_3((1,2)) = 9 > 2^3$ hence $(1,2)$ is a 1-losing 3-state, and so $\pi_1 = 1$. For $L>1$, it seems one must resort to an exhaustive search in order to find π_L. We have computed the first few values:

$$\{\pi_L\}_{L=1}^{\infty} = \{1, 2, 4, 7, \ldots\}$$

A directly computable upper bound $\mu_L \ge \pi_L$ is obtained via the generalized volume bound, by finding the minimal positive integer μ_L for which

$$V_{2\mu_L+1}((0^{\mu_L-1}, L, L+1)) > L \cdot 2^{2\mu_L+1}$$

Practicing some algebra, we get a simpler expression:

$$\mu_L = \inf\left\{\mu \in \mathbb{N} \,:\, 2^{2\mu} > L\binom{2\mu+1}{\mu}\right\} \quad (5)$$

It can be shown the expression above is well defined (i.e., μ_L is finite for any L), and in fact $\mu_L = \mathrm{O}(L^2)$. However, for small L we get $\{\mu_L\}_{L=1}^{\infty} = \{1, 4, 11, 20, \ldots\}$, so this bound seems far from tight.

Theorem 3 (Generalized Translation Property): Let $n \ge 2\pi_L+1$. If $\boldsymbol{s}$ is a Λ_L-winning n-state and $s^{(\pi_L-1)} \ge 2L+1$, then $T^{\pi_L}\boldsymbol{s}$ is a Λ_L-winning $n-(2\pi_L+1)$-state.

Proof: First we prove for $n = 2\pi_L+1$. Assume that $\boldsymbol{s}$ is a Λ_L-winning $(2\pi_L+1)$-state and $s^{(\pi_L-1)} \ge 2L+1$, but $T^{\pi_L}\boldsymbol{s}$ is not a Λ_L-winning 0-state. Therefore, it must be that $s^{(\pi_L)} \ge L+1$. Since we also have $s^{(\pi_L-1)} \ge 2L+1$, then $\boldsymbol{s}$ dominates the state $(0^{\pi_L-1}, L, L+1)$ and so the latter must be a L-winning $(2\pi_L+1)$-state, which by the definition of π_L results in a contradiction. Thus, $T^{\pi_L}\boldsymbol{s}$ is a Λ_L-winning 0-state, proving the result for $n = 2\pi_L+1$.

We now proceed by induction. Assume the result holds for all $k<n$, and let $\boldsymbol{s}$ be a Λ_L-winning n-state with $s^{(\pi_L-1)} \ge 2L+1$. Then there exists a partition $\boldsymbol{s} = \boldsymbol{a}+\boldsymbol{b}$ so that both $\boldsymbol{a}+T\boldsymbol{b}$ and $T\boldsymbol{a}+\boldsymbol{b}$ are Λ_L-winning $(n-1)$-states. If both these states satisfy the conditions of the Theorem, then by the induction assumption

$$\begin{aligned} \boldsymbol{x} &\triangleq T^{\pi_L}(T\boldsymbol{a}+\boldsymbol{b}) = T(T^{\pi_L}\boldsymbol{a}) + T^{\pi_L}\boldsymbol{b} \\ \boldsymbol{y} &\triangleq T^{\pi_L}(\boldsymbol{a}+T\boldsymbol{b}) = T^{\pi_L}\boldsymbol{a} + T(T^{\pi_L}\boldsymbol{b}) \end{aligned}$$

are both Λ_L-winning $(n-1-(2\pi_L+1))$-states. However, $T^{\pi_L}\boldsymbol{a}$ and $T^{\pi_L}\boldsymbol{b}$ are a valid partition of $T^{\pi_L}\boldsymbol{s}$, hence the latter

[2] If $\boldsymbol{s}^{(0)} < 2L$ then we set $B_L\boldsymbol{s} = \boldsymbol{s}$.

[3] Note that some care should be taken here in the selection of the initial state, and a sequence $R_n \to R$ should be considered.

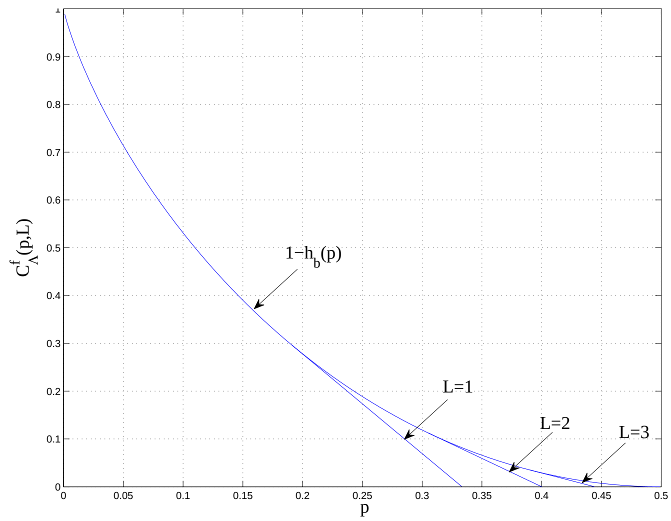

Fig. 1. Upper bounds on $C_\Lambda^f(p, L)$ for various values of the list size L.

can be reduced to $\boldsymbol{x}, \boldsymbol{y}$, which implies it is a Λ_L-winning $n-(2\pi_L+1)$-state, as desired. To conclude, suppose (without loss of generality) that $\boldsymbol{a}+T\boldsymbol{b}$ does not satisfy the conditions of the Theorem. Hence, it must be that $a^{(\pi_L-1)} + b^{(\pi_L)} \leq 2L$, which in particular implies that $s^{(\pi_L)} \leq 2L$. We therefore have that $T^{\pi_L}\boldsymbol{s} = T^{\pi_L}B_L\boldsymbol{s}$, and since $s^{(\pi_L-1)} \geq 2L+1$ we also have that $(B_L\boldsymbol{s})^{(0)} = 2L$. The latter implies that $B_L\boldsymbol{s} = \boldsymbol{t}_{j,k,L}$ for some $j, k \geq 0$, and using Lemma 3

$$V_{j+k+1}(\boldsymbol{s}) > V_{j+k+1}(B_L\boldsymbol{s}) = L \cdot 2^{j+k+1}$$

hence $n \geq j+k+2$. However, as an immediate implication of Lemma 3 we have that $T^{\pi_L}B_L\boldsymbol{s}$ is a L-winning $(j+k+1-2\pi_l)$-state, and due to its structure it is in particular also a Λ_L-winning $(j+k+1-2\pi_l)$-state. We have already seen that $T^{\pi_L}\boldsymbol{s} = T^{\pi_L}B_L\boldsymbol{s}$, and therefore $T^{\pi_L}\boldsymbol{s}$ must be a Γ_L-winning $(n-1-2\pi_l)$-state, as required. ∎

This result can be interpreted as follows: If Ulam's game with t lies can be won with n questions under a list-of-L and using only Λ_L strategies, then the game with $t-\pi_L$ lies can be won using only $n-(2\pi_L+1)$ questions. It should be noted that in its current form, the generalized translation property does not hold if Λ_L-winning is replaced with L-winning, i.e., when all game strategies are allowed. One extreme counterexample is the state $\boldsymbol{s} = (0, 0, 1, 4)$ which is not Λ_2-winning n-state for any n, but is a borderline 2-winning 8-state while its corresponding translation $T^{\pi_2}\boldsymbol{s} = (1, 4)$ is a borderline 2-winning 4-state (and also a borderline Λ_2-winning 4-state).

IV. An Upper Bound

In this section, the generalized volume bound and translation property are combined to derive an upper bound on $C_\Lambda^f(p, L)$. The bound is depicted in Figure 1 for several values of L.

Theorem 4: The following upper bound holds

$$C_\Lambda^f(p, L) \leq \begin{cases} 1 - h_b(p) & 0 \leq p \leq p_L \\ a_L\left(1 - \frac{2\pi_L+1}{\pi_L}p\right) & p_L \leq p \leq \frac{\pi_L}{2\pi_L+1} \\ 0 & p \geq \frac{\pi_L}{2\pi_L+1} \end{cases} \tag{6}$$

where a_L, p_L are such that the straight line in (6) is tangent to $1-h_b(p)$ at p_L.

Proof: The Hamming bound is a direct consequence of the generalized volume bound of Theorem 1. A necessary condition for the initial state $\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}$ to be a L-winning (and in particular Λ_L-winning) n-state, is given by

$$L \cdot 2^n \geq V_n(\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}) = \lceil 2^{nR}\rceil \sum_{k=0}^{\lceil np\rceil} \binom{n}{k} \tag{7}$$

and therefore any achievable rate must satisfy for all large n

$$R \leq 1 - \frac{1}{n}\log \sum_{k=0}^{\lceil np\rceil}\binom{n}{k} + \frac{\log L}{n} \underset{n\to\infty}{\longrightarrow} 1 - h_b(p) \tag{8}$$

This bound of course holds for $C^f(p, L)$ as well, for all $p < \frac{1}{2}$.

Let us now derive the tangential bound. Using the generalized translation property of Theorem 3, a necessary condition for $\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}$ to be a Λ_L-winning n-state is that $T^{\alpha n\pi_L}\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}$ is a Λ_L-winning $(n(1-(2\pi_L+1)\alpha))$-state, for any selection of $0 < \alpha < \frac{p}{\pi_L}$ (up to minor integer issues, and assuming $p < \frac{\pi_L}{2\pi_L+1}$). Now, the state $T^{\alpha n\pi_L}\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}$ must satisfy the generalized volume bound:

$$L \cdot 2^{n(1-(2\pi_L+1)\alpha)} \geq V_{n(1-(2\pi_L+1)\alpha)}\left(T^{\alpha n\pi_L}\boldsymbol{I}_{\lceil 2^{nR}\rceil}^{\lceil np\rceil}\right)$$
$$= \lceil 2^{nR}\rceil \sum_{k=0}^{n(p-\alpha\pi_L)} \binom{n(1-(2\pi_L+1)\alpha)}{k}$$

Taking the logarithm of both sides and letting $n \to \infty$, results in

$$R \leq (1-(2\pi_L+1)\alpha)\cdot\left(1 - h_b\left(\frac{p-\alpha\pi_L}{1-(2\pi_L+1)\alpha}\right)\right)$$

Introducing a change of variables $\beta = \frac{p-\alpha\pi_L}{1-(2\pi_L+1)\alpha}$, this reduces to

$$R \leq \frac{1-\frac{2\pi_L+1}{\pi_L}p}{1-\frac{2\pi_L+1}{\pi_L}\beta}\cdot(1-h_b(\beta)) \triangleq f(p\,;\beta, L) \tag{9}$$

Fixing β, the above bound holds for any $\beta < p < \frac{\pi_L}{2\pi_L+1}$. As a function of p, we have that $f(p\,;\beta, L)$ is a straight line with a negative slope, intersecting the horizontal axis at $p = \frac{\pi_L}{2\pi_L+1}$, as desired. Therefore, to get the best bound we need to find the value of β minimizing the slope, which can be found be solving $\frac{\partial^2 f}{\partial p\partial\beta} = 0$. This results in

$$\left(\beta - \frac{\pi_L}{2\pi_L+1}\right)\log\left(\frac{\beta}{1-\beta}\right) = 1 - h_b(\beta) \tag{10}$$

Practicing some algebra, we find that the optimal β is the unique root β_0 of the polynomial

$$\beta^{\pi_L}(1-\beta)^{\pi_L+1} - 2^{-(2\pi_L+1)} \tag{11}$$

which satisfies $0 < \beta_0 < \frac{\pi_L}{2\pi_L+1}$. We can now set $a_L = \frac{1-h_b(\beta_0)}{1-\frac{2\pi_L+1}{\pi_L}\beta_0}$, and to conclude the proof we show that $f(p\,;\beta_0, L)$ is tangent to the Hamming bound at the point $p_L = \beta_0$.

To that end, note first that $f(\beta_0\,;\beta_0, L) = 1 - h_b(\beta_0)$, namely the straight line coincides with the hamming bound at β_0. The slope of the hamming bound at this point is given by

$$\frac{d}{dp}(1-h_b(p))\Big|_{p=\beta_0} = \log\left(\frac{\beta_0}{1-\beta_0}\right) = \frac{1-h_b(\beta_0)}{\beta_0 - \frac{\pi_L}{2\pi_L+1}} \quad (12)$$

where in the second transition we have used the fact that β_0 satisfies (10). But the right-hand-side of (12) is just the slope of $f(p\,;\beta_0, L)$. ∎

V. Discussion

In this paper we addressed the problem of error correction with feedback under list decoding, and its equivalent statement as a variant of Ulam's game. We made some initial progress by providing Berlekamp-type constraints on the structure of winning strategies for the game, and using those to derive a preliminary result in the form of an upper bound on $C^f_\Lambda(p, L)$, the best achievable rate for error correction with feedback under list-of-L decoding and a maximal error fraction p, for a large family of strategies. This latter major shortcoming of our result stems from the fact that the generalized translation property was proved only under some additional assumptions on the type of eligible questions. It can be shown that the family of allowed strategies can be further enlarged in a natural way while still maintaining the generalized translation property. However, by the way of a counterexample, it was demonstrated that the property as stated does not hold in general. It remains to be explored whether such a property can at all hold without any restriction on game strategies, under some further assumptions on the state structure.

The above being said, it should be emphasized that the constraint on eligible strategies under which our bound holds is rather weak, in the sense of posing a restriction roughly only on how the bottom $2L$ objects in the state vector of the game are to be partitioned. There is some reason to believe that the partition of the bottom objects becomes an important issue only at the very last rounds of the game, and so our restrictions might incur only a small loss in the number of questions required to win, for states amenable to Λ_L strategies. A reasonable direction to pursue would therefore be to show that (roughly) for any L-winning n-state there exists some dominating Λ_L-winning $(n + \mathrm{o}(n))$-state. If such a statement can indeed be proved, then the gap introduced by our restrictions will become asymptotically negligible, and our bounds on $C^f_\Lambda(p, L)$ will immediately hold for $C^f(p, L)$ as well. This however remains an open question, and an upper bound for $C^f(p, L)$ is still to be pursued.

Another important path for future research is the question of achievability. It is already known that for a list-of-1, our upper bound on $C^f_\Lambda(p, 1)$ in fact coincides with $C^f(p, 1)$ [2][15], and therefore trivially serves as a lower bound for $C^f(p, L)$. The achievability of the convex part in $C^f(p, 1)$ has been proved via an adaptation of the Horstein scheme [9], and it should be further examined if this approach can be generalized to the convex part of the $C^f_\Lambda(p, L)$ bound. The achievability of the tangential bound was originally proved for a list-of-1 by recursively constructing a table of winning states [2]. However, a recently suggested explicit strategy achieving the same end [1], may provide some insight possibly applicable in the list-of-L case as well. Finally, it is interesting to note that if the convex part of the bound turns out to be tight, then feedback will allow a stronger statement of approachability to the Hamming bound via list-decoding: While in the absence of feedback the Hamming bound is approached only in the limit of $L \to \infty$ [3], proving the convex part of the bound is tight will imply that when feedback is available, then for any given $p < \frac{1}{2}$ there exists a *finite* L for which the Hamming bound is achievable.

References

[1] R. Ahlswede, C. Deppe, and V. Lebedev. Binary error correcting codes with noiseless feedback, localized errors, or both. *Comb. and Algo. Found. of Pat. and Ass. Disc*, 2006.

[2] E. R. Berlekamp. *Block Coding with Noiseless Feedback*. doctoral dissertation, MIT, 1964.

[3] V.M. Blinovsky. Bounds for codes in the case of list decoding of finite volume. *Prob. Inform. Trans.*, 22(1):7–19, 1986.

[4] C. Deppe. Solution of ulam's searching game with three lies or an optimal adaptive strategy for binary three-error-correcting codes. *Discrete Math.*, 224(1-3):79–98, 2000.

[5] C. Deppe. *Coding with Feedback and Searching with Lies*, book chapter in *Entropy, Search, Complexity*, volume 16 of *Bolyai Society Mathematical Studies*, pages 27–70. Springer Berlin Heidelberg, 2007.

[6] D.L Desjardins. *Precise Coding with Noiseless Feedback*. doctoral dissertation, MIT, 2002.

[7] P. Elias. Error correcting codes for list decoding. *IEEE Trans. Info. Theory*, 37:5 – 12, January 1991.

[8] V. Guruswami. *List Decoding of Error-Correcting Codes*. doctoral dissertation, MIT, 2001.

[9] M. Horstein. Sequential transmission using noiseless feedback. *IEEE Trans. Info. Theory*, IT-9:136–143, JUL 1963.

[10] F.J. MacWilliams and N.J.A. Sloane. *Theory of Error-correcting Codes*. Elsevier Science & Technology, 1977.

[11] A. Pelc. Solution of ulam's problem on searching with a lie. *J. Comb. Theory Ser. A*, 44(1):129–140, 1987.

[12] C.E. Shannon. The zero-error capacity of a noisy channel. *IRE. Trans. Info. Theory*, IT-2:8–19, 1956.

[13] J. Spencer. Ulam's searching game with a fixed number of lies. *Theor. Comput. Sci.*, 95(2):307–321, 1992.

[14] S.M. Ulam. *Adventures of a Mathematician*. Charles Scribner's Sons, New York, 1976.

[15] K. Sh. Zigangirov. Number of correctable errors for transmission over a binary symmetrical channel with feedback. *Prob. Inform. Trans.*, 12:85–97, 1976.