Journal of Combinatorial Theory, Series A 116 (2009) 1253–1270

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Two-batch liar games on a general bounded channel

Robert B. Ellis [a], Kathryn L. Nyman [b]

[a] Department of Applied Mathematics, Illinois Institute of Technology, Chicago, IL 60616, United States
[b] Department of Mathematics and Statistics, Loyola University Chicago, Chicago, IL 60626, United States

ARTICLE INFO

Article history:
Received 7 May 2008
Available online 10 April 2009

Keywords:
Rényi–Ulam game
Liar game
Pathological liar game
Adaptive coding
Searching with lies
Unidirectional errors

ABSTRACT

We consider an extension of the 2-person Rényi–Ulam liar game in which lies are governed by a channel C, a set of allowable lie strings of maximum length k. Carole selects $x \in [n]$, and Paul makes t-ary queries to uniquely determine x. In each of q rounds, Paul weakly partitions $[n] = A_0 \cup \cdots \cup A_{t-1}$ and asks for a such that $x \in A_a$. Carole responds with some b, and if $a \neq b$, then x accumulates a lie (a,b). Carole's string of lies for x must be in the channel C. Paul wins if he determines x within q rounds. We further restrict Paul to ask his questions in two off-line batches. We show that for a range of sizes of the second batch, the maximum size of the search space $[n]$ for which Paul can guarantee finding the distinguished element is $\sim t^{q+k}/(E_k(C)\binom{q}{k})$ as $q \to \infty$, where $E_k(C)$ is the number of lie strings in C of maximum length k. This generalizes previous work of Dumitriu and Spencer, and of Ahlswede, Cicalese, and Deppe. We extend Paul's strategy to solve also the pathological liar variant, in a unified manner which gives the existence of asymptotically perfect two-batch adaptive codes for the channel C.

1. Introduction

We consider a generalization of the Rényi–Ulam liar game, originating in [1] and [2]. In this 2-player "20 questions" game, Paul may ask 20 Yes–No questions in order to identify a distinguished element x from a set $[n] := \{1, \ldots, n\}$, where Carole answers "Yes" or "No" and is allowed to lie at most once. If Paul is allowed q questions, he can identify x provided $n \lesssim 2^q/(q+1)$ (see [3]). Restricting Carole to always tell the truth reduces the game to binary search. An equivalent coding theoretic formulation is block coding over a noisy binary symmetric channel with noiseless feedback [4].

E-mail addresses: rellis@math.iit.edu (R.B. Ellis), knyman@math.luc.edu (K.L. Nyman).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2009.03.005

The basic Rényi–Ulam liar game has these parameters: search space $[n]$, number of questions q, and Carole's maximum number of lies k. In [5], Dumitriu and Spencer determined the first-term asymptotics of the following extension: instead of binary Yes–No questions, Paul asks t-ary questions, and Carole has a set of lie types (e.g., "Yes" when the truth is "No") from which she may draw up to k times with repetition. Furthermore, Paul asks his questions in two batches, receiving Carole's answers at the end of a batch. In [6], Ahlswede, Cicalese, and Deppe extended this result to weighted lies, with bounded total weight. In [7], the first author and Yan introduced the pathological variant of the liar game, in which Paul wins provided at least one element in the search space survives being eliminated, with Carole playing adversely.

In this paper, we simultaneously unify and extend [5–7] as follows. Our channel is a finite list of strings of lies of varying type, from which Carole selects one string to apply its lies in order and interspersed among her responses. Every candidate $y \in [n]$ has a game lie string generated by Carole's q responses from the perspective of y being the element Paul seeks; if y's string is not in the list, then y is eliminated from the search space. Furthermore, Paul is constrained to the aforementioned two-batch question strategy. We solve asymptotically both the original and the pathological variants for the optimal n for which Paul can win in terms of q, giving unified winning strategies for Paul in the original and pathological variants which correspond to asymptotically perfect adaptive codes. This, our main result, is given as Theorems 2.3–2.4 in Section 2.1, with proofs deferred to Section 3, followed by concluding remarks in Section 4. A list of principal notation appears in Table 1 after Section 2, and the beginning of Section 3.2 is a technical outline of Paul's unified winning strategies.

Our general channel condition is natural because it encompasses the previously studied binary and t-ary liar games on a symmetric, asymmetric, or weighted channel. It also specializes to the binary unidirectional channel, in which lies may be of one type or the other but not mixed (see Example 2.5); for a bounded number of lies in arbitrary position, we believe that the most general previous result is [6]. Furthermore, the pathological variant appears to be less studied, with results only in the binary asymmetric and binary symmetric cases [7,8]. Finally, requiring Paul to ask questions in two batches with a range of possible sizes for the second batch provides intuition about the fully nonadaptive one-batch case, which includes k-error-correcting codes and radius k covering codes, in the original and pathological variants, respectively.

2. Definitions and main result

The Rényi–Ulam liar game is a 2-player perfect information game with integer parameters $n, q, k \geqslant 0$ and $t \geqslant 2$, played over a t-ary communication channel C of order k, which we now define. The *lies* for the alphabet $T := \{0, \ldots, t-1\}$ are the set

$$\mathcal{L}(t) := \big\{(a,b) \in T \times T\colon\ a \neq b\big\}.$$

A *lie string* is a finite ordered list of lies, that is, an element of the language $\mathcal{L}(t)^* := \bigcup_{i \geqslant 0} \mathcal{L}(t)^i$. For our purposes, a *$t$-ary communication channel of order k* is an arbitrary subset

$$C \subseteq \bigcup_{i=0}^{k} \mathcal{L}(t)^i,$$

such that $C \cap \mathcal{L}(t)^k \neq \emptyset$, representing the usable lie strings of the game. We denote the order of C by $o(C)$. The unique element and *empty string* ϵ of $\mathcal{L}(t)^0$ may or may not be in C. The *length* $|u|$ of $u \in \mathcal{L}(t)^*$ is simply the number of lies in u. The *concatenation* of $u, v \in \mathcal{L}(t)^*$ is defined as $uv := (a_1, b_1) \cdots (a_{j'}, b_{j'})$ when $u = (a_1, b_1) \cdots (a_j, b_j)$ and $v = (a_{j+1}, b_{j+1}) \cdots (a_{j'}, b_{j'})$.

Paul and Carole play a q-round game on the set $[n] := \{1, \ldots, n\}$. Each $y \in [n]$ begins the game with lie string ϵ. To start each round, Paul weakly partitions $[n]$ into t parts by choosing a *question* $(A_0, \ldots, A_{t-1})$ such that $[n] = A_0 \dot\cup \cdots \dot\cup A_{t-1}$, where $\dot\cup$ denotes disjoint union. Carole completes the round by responding with her *answer*, an index $j \in T$. If $y \in A_j$, then y accumulates no lie. Otherwise $y \in A_i$ for some $i \neq j$, and (i, j) is post-pended to y's current lie string. The *game response string* is the ordered sequence $w'_1 \cdots w'_q \in T^q$ of Carole's responses. The *game lie string* for y is its final accumulated sequence of lies $(a_1, b_1)\cdots(a_j, b_j) \in \bigcup_{i=0}^{q} \mathcal{L}(t)^i$. By definition, the b_i's must appear, in order, as a substring of the game response string.

$$\begin{array}{ll} \text{Truthful response string for } y\text{:} & w_1 \cdots w_{i_1} \cdots w_{i_\ell} \cdots w_{i_j} \cdots w_q \\ \text{Game lie string for } y\text{:} & \begin{array}{c} a_1 \ \cdots \ a_\ell \ \cdots \ a_j \\ b_1 \ \cdots \ b_\ell \ \cdots \ b_j \end{array} \\ \text{Game response string:} & w'_1 \cdots w'_{i_1} \cdots w'_{i_\ell} \cdots w'_{i_j} \cdots w'_q \end{array} \tag{1}$$

Here, $w_{i_\ell} = a_\ell$ and $w'_{i_\ell} = b_\ell$ for all $1 \leqslant \ell \leqslant j$, and $w_i = w'_i$ for all other indices. If y's game lie string is in C, then y *survives* the game; otherwise y is *disqualified* (*eliminated*). More broadly, at any given round, y survives iff its final lie string might still be in C. Rather than requiring Carole to choose x at the beginning, we equivalently allow her to update her choice of x, lie string, and game response string at any time. Paul wins the *original variant* iff after q rounds at most one element (candidate for x) survives, and he wins the *pathological variant* iff after q rounds at least one element survives. For the second variant, we think of a capricious Carole lying "pathologically" in order to eliminate all elements as quickly as possible. Carole plays an adversarial strategy in both variants and wins if Paul does not. In a *fully adaptive* game, Paul receives Carole's answer each round before forming his next question. We will usually restrict Paul to a *two-batch strategy* consisting of q_1 questions in the first batch and q_2 questions in the second batch. Carole responds to an entire batch at once after receiving all questions in the batch.

Definition 2.1. The (n, q_1, q_2, C)*-game* is the two-batch original liar game with search space $[n]$ on a t-ary channel C of order $o(C) < \infty$, with q_1 and q_2 questions in the first and second batches, respectively. The $(n, q_1, q_2, C)^*$*-game* is the two-batch pathological liar game with the same parameters.

For the binary channel $C = \{(0, 1)\}$, Carole must lie since $\epsilon \notin C$. But Paul may win the original variant regardless of $[n]$ by setting $A_0 = \emptyset$ and $A_1 = [n]$ every round. To avoid such trivial winning strategies, we constrain C as follows.

Definition 2.2 *(Non-degenerate channel).* The channel C is *non-degenerate* with respect to the original variant provided either

(1) $\epsilon \in C$, or
(2) for all $a \in T$, there exists a lie string $u \in C$ with $u = (a, b_1)\cdots(a, b_j)$;

and is *non-degenerate* with respect to the pathological variant provided either

(1) $\epsilon \in C$, or
(2) for all $b \in T$, there exists a lie string $u \in C$ with $u = (a_1, b)\cdots(a_j, b)$.

In the above example, $C = \{(0, 1)\}$ had no u of the form $(1, b_1)\cdots(1, b_j)$. In the pathological variant, unless C is non-degenerate there exists $b \in T$ with no $u \in C$ of the form $(a_1, b)\cdots(a_j, b)$. Carole wins regardless of $[n]$ by always answering b, thereby eliminating every $y \in [n]$. The fully adaptive case needs a more careful definition of non-degeneracy (though $\epsilon \in C$ suffices), which we leave to future work.

2.1. The main result

For a t-ary channel C of order k and for $0 \leqslant j \leqslant k$, define the number

$$E_j(C) := \left|C \cap \mathcal{L}(t)^j\right|$$

of length j lie strings in C. Our main result is that, for q_2 sufficiently bounded, the asymptotic optimal n for which Paul can win the (n, q_1, q_2, C)-game or $(n, q_1, q_2, C)^*$-game depends on $E_k(C)$ and not on C itself. For convenience, we separate the main result into bounds for Paul and bounds for Carole.

Theorem 2.3. *Let C be an order k channel, let $f(q)$ be nonnegative with $f(q) \to \infty$, and let $q_1 + q_2 = q$. There exist constants c_1, c_2 such that if $(\ln q)^{3/2} f(q) \leqslant q_2 \leqslant c_1 q^{k/(2k-1)}$ and*

$$n \leqslant \frac{t^{q+k}}{E_k(C)\binom{q}{k}}\left(1 - c_2\frac{\sqrt{\ln q}}{q_2^{1/3}}\right), \tag{2}$$

then, for q large enough, Paul can win the (n, q_1, q_2, C)-game. If, in addition, C is non-degenerate with respect to the pathological variant, then there exists a constant c_3 such that if $(\ln q)^{3/2} f(q) \leqslant q_2 \leqslant c_1 q^{k/(2k-1)}$ and

$$n \geqslant \frac{t^{q+k}}{E_k(C)\binom{q}{k}}\left(1 + c_3\frac{\sqrt{\ln q}}{q^{1/3}}\right), \tag{3}$$

then, for q large enough, Paul can win the $(n, q_1, q_2, C)^*$-game.

Theorem 2.4. *Let C be an order k channel, let $f(q)$ be nonnegative with $f(q) \to \infty$, and let $q_1 + q_2 = q$ with $\max(q_1, q_2) \gg \min(q_1, q_2) \geqslant (\ln q)^{3/2} f(q)$. There exist constants c_4, c_5 such that if C is non-degenerate with respect to the original variant and*

$$n \geqslant \frac{t^{q+k}}{E_k(C)\binom{q}{k}}\left(1 + \frac{c_4 \min(q_1, q_2)}{q} + c_5\frac{\sqrt{\ln q}}{\max(q_1, q_2)^{1/3}}\right),$$

then, for q sufficiently large, Carole can win the (q_1, q_2, n, C)-game. Regardless of the choice of q_1 and q_2, there exists a constant c_6 such that if

$$n \leqslant \frac{t^{q+k}}{E_k(C)\binom{q}{k}}\left(1 - \frac{c_6\sqrt{\ln q}}{q^{1/3}}\right),$$

then, for q sufficiently large, Carole can win the $(q_1, q_2, n, C)^*$-game.

The above constants depend on k but not on q, q_1, or q_2. We defer proofs until Section 3. The proof of Theorem 2.3 builds on that of Theorem 1.2 of [5], which gives the optimal n, up to the first asymptotic term in q, for which Paul can win the original game variant when $C = \bigcup_{j=0}^{k} \mathcal{L}'(t)^j$, for some fixed $\mathcal{L}'(t) \subseteq \mathcal{L}(t)$. We borrow their two-batch structure, but extend it to handle a more general channel, the pathological game variant, and a wider range of second batch size q_2. Most original is our unified treatment in the key Theorem 3.8 of Paul's winning strategies in both variants, which proves the existence of asymptotically perfect adaptive codes for any non-degenerate channel C. These codes correspond to packings within coverings of the t-ary hypercube T^q of the sets of game response strings for which individual elements of the search space survive (like Hamming balls for nonadaptive codes). Our proof for when Carole has a winning strategy borrows from [5] but applies the two-batch structure in the original variant as is necessary to be consistent with the definition of a non-degenerate channel. A motivation for our definition of C was the following example.

Example 2.5. In a liar game over a binary asymmetric (Z-)channel, Carole may lie with "Yes" when the correct answer is "No" but not vice-versa. In the companion asymmetric channel, only a "No" to "Yes" lie is allowed. The 2-lie unidirectional channel $C = \{\epsilon, (0,1), (0,1), (0,1)(0,1), (1,0)(1,0)\}$ may be interpreted as Paul knowing that the game is being played over one of the asymmetric channels with $k = 2$, but not which. In prior work on the fully nonadaptive case (e.g., [9,10]), C is called the "unidirectional error" channel.

Substantially more general channels are possible. For example, by setting $C = \{(0,1), (1,0), (0,1)(1,0), (1,0)(0,1)\}$, we force Carole to lie (as $\epsilon \notin C$), and require that if she lies twice, her second lie must be of the opposite type.

2.2. Suffix channels and the game state vector

At any given round in the game, an element $y \in [n]$ has accumulated a partial game lie string $u \in \mathcal{L}(t)^*$. We define the *suffix channel* $S_C(u)$ to be the set of all ways to extend to a game lie string in the channel. Formally,

$$S_C(u) := \{v\colon\ uv \in C\} \quad \text{and} \quad \mathcal{S}(C) := \{S_C(u)\colon\ u \in \mathcal{L}(t)^*\}$$

is the set of suffix channels of C. Disqualified elements $y \in [n]$ have suffix channel $\emptyset$. We track each $y \in [n]$ via its suffix channel at any given round.

Definition 2.6. The *game state vector* after a given round in the original or pathological game is the vector $(x_{C'}\colon\ C' \in \mathcal{S}(C))$ indexed by the suffix channels of C, where $x_{C'}$ counts the number of elements of $[n]$ whose accumulated lie string u satisfies $S_C(u) = C'$. The *coarsened state vector*, $(x_0, x_1, \ldots, x_k)$, is obtained from the game state vector by grouping elements with suffix channels of the same order, so that

$$x_i := \sum_{\substack{C' \in \mathcal{S}(C) \\ o(C') = k-i}} x_{C'} \quad \text{for } 0 \leqslant i \leqslant k.$$

At the start of our game, $x_C = n$ and $x_{C'} = 0$ for $C' \neq C$. If, after $q' \leqslant q$ rounds, $y \in [n]$ has partial game lie string u, y survives the entire game iff y survives the game on the last $q - q'$ rounds with respect to the suffix channel $S_C(u)$. The element y has been disqualified after $q' \leqslant q$ rounds iff $S_C(u) = \emptyset$ or $q - q' < \min\{|v|\colon\ v \in S_C(u)\}$, that is, if there are no strategies of questions by Paul and answers by Carole in the last $q - q'$ rounds in which the partial lie string of y can be completed to obtain a game lie string in C. Thus we have the following.

Lemma 2.7. *Let $0 \leqslant q_1 \leqslant q$ and $q_1 + q_2 = q$. Given that the state vector is $(x_{C'}\colon\ C' \in \mathcal{S}(C))$ after q_1 rounds, Paul wins the entire game, in either variant, iff he wins the q_2-round game starting with state vector $(x_{C'}\colon\ C' \in \mathcal{S}(C))$.*

The state vector after q_1 rounds is a snapshot of the game regardless of adaptive or two-batch questioning. Setting $q_1 = q$, Paul wins the original (pathological) variant iff after q rounds $\sum_{C',\,\epsilon \in C'} x_{C'} \leqslant 1$ ($\geqslant 1$), as the empty lie string must be in an element's suffix channel for it to survive with no questions left.

We conclude with channel statistics needed in Theorem 3.8. The number of prefixes u of an order i suffix channel of C is $p_i(C) := |\{u \in \mathcal{L}(t)^*\colon\ o(S_C(u)) = i\}|$. Refining $p_i(C)$ by the length of u, set $p_i^{(j)}(C) := |\{u \in \mathcal{L}(t)^j\colon\ o(S_C(u)) = i\}|$. Note that $p_i^{(j)}(C) = 0$ when $j > k - i$, and that $p_i(C) = \sum_{j=0}^{k-i} p_i^{(j)}(C)$.

3. Proof of the main result

We begin with a notion of balanced strings of T^q that have nearly equal frequencies of each letter of T. All game response strings for which a typical $y \in [n]$ survives will be balanced. For a 1-batch game, this set is a C-shadow, which is generalized in Section 3.1 from a Hamming ball. In Section 3.2, Paul's winning strategies for both variants combine shadows from the first batch with those from the second batch through suffix channels in order to analyze the overall set of game response strings for which any $y \in [n]$ survives. Theorem 3.8 gives winning conditions for Paul in both variants in terms of a packing within a covering of collections of these sets. The non-existence of such a packing (resp., covering) provides a winning condition for Carole in the original (resp., pathological) variant, in Theorem 3.9 of Section 3.3. Section 3.5 converts these winning conditions into the main asymptotic results, Theorems 2.3–2.4, after developing a generalized Varshamov bound in Section 3.4.

Table 1
Principal notation.

$[n]$, y	search space $[n] := \{1, \ldots, n\}$ and typical element $y \in [n]$
q, q_1, q_2	number of total, first batch, and second batch questions, resp.
$(A_0, \ldots, A_{t-1})$	t-ary question by Paul weakly partitioning $[n]$, where $t \geqslant 2$
T^Q	response strings $\{0, \ldots, t-1\}^Q$ for a batch of Q questions
$(a, b) \in T \times T$	w.r.t. some y, truth a and response b; a "lie" when $a \neq b$
$\mathcal{L}(t)$, $\mathcal{L}(t)^i$	set of all lies of $T \times T$, and of all lie strings of length i
$C \subseteq \bigcup_{i=0}^{k} \mathcal{L}(t)^i$	t-ary channel of order $o(C) = k$, with $C \cap \mathcal{L}(t)^k \neq \emptyset$
$u \in \mathcal{L}(t)^*$	usually, the accumulated lie string of some $y \in [n]$
$uv \in C$	lie string of surviving y; u, v from first, second batches, resp.
w, w'	truthful response string for some y, actual response string
z, z'	same as previous but usually for second batch
$S_C(u)$	suffix channel of u, the set of v with $uv \in C$ a legal lie string
$x_{C'}$, x_i	counts $y \in [n]$ surviving with suffix channel C', $o(C') = k - i$
(M, r)-balanced	all $w \in T^Q$ with $\leqslant \frac{1}{t}\lceil Q/M \rceil + r$ per section of each letter of T
$T^Q(M, r)$	set of (M, r)-balanced strings of T^Q
$\{w' \colon w \xrightarrow{u} w'\}$	set of all w' arising from w under application of u as in (1)
$B(w, C)$	C-shadow with stem w; union over $u \in C$ of $\{w' \colon w \xrightarrow{u} w'\}$
$(x_{C'} \colon C' \in \mathcal{S}(C))$	intra-batch state vector indexed by all suffix channels C'
$(x_i \colon 0 \leqslant i \leqslant k)$	previous vector additively grouped by $i = k - o(C')$
α	number of y Paul assigns to each $T^{q_1}(M_1, r_1)$, original variant
α'	additional number of y for previous, pathological variant
$A_t(Q, 2j+1)$	maximum size of a t-ary length Q code with packing radius j

Definition 3.1. Let $t \geqslant 2$ and $Q, M > 0$ be integers, and let $r > 0$. A string $w \in T^Q$ is (M, r)-*balanced* if, after splitting w into M contiguous substrings of nearly equal length with (for definiteness) length $\lceil Q/M \rceil$ substrings preceding length $\lfloor Q/M \rfloor$ substrings, each letter of T appears in each section at most $\frac{1}{t}\lceil Q/M \rceil + r$ times. If w is not (M, r)-balanced, it is (M, r)-*unbalanced*. Define $T^Q(M, r)$ to be the set of (M, r)-balanced strings of T^Q.

The Chernoff bound applies to the number of (M, r)-balanced strings in T^Q.

Lemma 3.2. *Let $t \geqslant 2$ and $Q, M > 0$ be integers, and let*

$$r(Q, M, i) = \sqrt{\left\lceil \frac{Q}{M} \right\rceil \frac{\ln(Mt2^i)}{2}}. \tag{4}$$

Then for $i \geqslant 1$, fewer than $t^Q 2^{-i}$ strings in T^Q are $(M, r(Q, M, i))$-unbalanced.

Proof. Select $w \in T^Q$ uniformly at random. A fixed letter $a \in T$ appears independently with probability $1/t$ in each of the at most $\lceil Q/M \rceil$ positions of a fixed section of w. Letting Y be the total number of occurrences of a in this section, by the standard Chernoff bound in Theorem A.1.4 of [11], $\Pr(Y > \frac{1}{t}\lceil Q/M \rceil + r(Q, M, i)) < \exp(-2r^2(Q, M, i)/\lceil Q/M \rceil) = \frac{2^{-i}}{Mt}$. The result follows by subadditivity over t letters and M sections. □

3.1. *Coding theoretic definitions*

Let $j, Q \geqslant 0$ and let $w = w_1 \cdots w_Q$, $w' = w'_1 \cdots w'_Q \in T^Q$. The *Hamming ball* of radius j, or j-*ball*, centered at w is the set $B(w, j) := \{w' \colon 0 \leqslant d(w, w') \leqslant j\}$, where $d(w, w') := |\{i \colon w_i \neq w'_i\}|$ is the (Hamming) distance between w and w'. We define distance to a set as usual; for example, for any $w \in T^Q$, $d(w, T^Q(M, r)) := \min\{d(w, w') \colon w' \in T^Q(M, r)\}$ is the distance between w' and the set of (M,r)-balanced strings of T^Q. Our channel C requires a generalization of Hamming balls to C-shadows. Just as a j-ball is obtained from the center by changing up to j digits, a C-shadow is obtained from the stem w by applying a lie string $u \in C$ to w, as in (1) for the case in which Paul's questions are fully nonadaptive.

Definition 3.3. Let $w, w' \in T^Q$, and let $u \in \mathcal{L}(t)^j$. We write $w \xrightarrow{u} w'$ if the lie string $u = (a_1, b_1)\cdots(a_j, b_j)$ can be applied to w to obtain w' as in (1).

Definition 3.4. Let $w \in T^Q$, and let C be a channel. Then the C-*shadow* $B(w,C)$ with stem w is defined as

$$B(w,C) := \bigcup_{u\in C}\{w' \in T^Q\colon\ w \xrightarrow{u} w'\}.$$

Note that the j-ball $B(w,j)$ is a C-shadow with stem w and $C = \bigcup_{\ell=0}^{j}\mathcal{L}(t)^\ell$. A set $\{B(w,C)\}_{(w,C)}$ of shadows is a *packing* in T^Q if $B(w,C)\cap B(w',C') = \emptyset$ for all distinct pairs of shadows in the set. The set is a *covering* of T^Q if $\bigcup_{(w,C)} B(w,C) = T^Q$. An $(x_i\colon\ 0 \leqslant i \leqslant k)$-packing (-covering) is a simultaneous packing (covering) of T^Q with x_i i-balls for $0 \leqslant i \leqslant k$. Similarly, an $(x_{C'}\colon\ C' \in \mathcal{I})$-packing (-covering) is a simultaneous packing (covering) of T^Q with $x_{C'}$ C'-shadows for C' in some indexing set $\mathcal{I}$ of channels. For our purposes, $\mathcal{I} = \mathcal{S}(C)$. From coding theory, $A_t(Q, 2j+1)$ is the maximum number of j-balls in a packing of T^Q (see, for example, [12]). We define $b(Q,t,j)$ to be the size of any j-ball $B(w,j)$ in T^Q, which is independent of w. In particular,

$$b(Q,t,j) = \sum_{\ell=0}^{j}\binom{Q}{\ell}(t-1)^\ell. \tag{5}$$

We make the following abbreviations in controlling $|B(w,C)|$ for balanced w:

$$G(Q,M,r,j) := \binom{M+j-1}{j}\left(\frac{1}{t}\left\lceil\frac{Q}{M}\right\rceil + r + k\right)^j \quad\text{and}$$

$$H(Q,M,r,j) := \binom{M}{j}\left(\min\left(0, \frac{1}{t}\left\lceil\frac{Q}{M}\right\rceil - (t-1)r - 2 - k\right)\right)^j. \tag{6}$$

Here, r corresponds to the balance tolerance parameter $r(Q,M,i)$ in (4), and k must appear to handle stems w with $d(w, T^Q(M,r)) \leqslant k$.

Lemma 3.5. *Let C be a channel, let $w \in T^Q$ satisfy $d(w,s) \leqslant k$ for some (M,r)-balanced $s \in T^Q$, and let $u \in \mathcal{L}(t)^j$ be a lie string of length j. Then*

$$H(Q,M,r,j) \leqslant \left|\{w'\colon\ w \xrightarrow{u} w'\}\right|, \quad \left|\{w'\colon\ w' \xrightarrow{u} w\}\right| \leqslant G(Q,M,r,j), \quad \textit{and} \tag{7}$$

$$\sum_{j=0}^{o(C)}\sum_{\substack{u\in C\\|u|=j}} H(Q,M,r,j) \leqslant \left|B(w,C)\right| \leqslant \sum_{j=0}^{o(C)}\sum_{\substack{u\in C\\|u|=j}} G(Q,M,r,j). \tag{8}$$

Proof. Divide w and s into M contiguous sections as in Definition 3.1. By definition, the maximum letter frequency per section of an (M,r)-balanced $s \in T^Q$ is at most $\frac{1}{t}\lceil Q/M\rceil + r$, and by subtraction the minimum letter frequency per section is at least $\frac{1}{t}\lceil Q/M\rceil - (t-1)r - 2$. Since $d(w,s) \leqslant k$, add and subtract k respectively from these quantities to get corresponding bounds for w. For (7), we prove the bound on $|\{w'\colon\ w \xrightarrow{u} w'\}|$; the bound on $|\{w'\colon\ w' \xrightarrow{u} w\}|$ follows by replacing $u = (a_1,b_1)\cdots(a_j,b_j)$ with $u' = (b_1,a_1)\cdots(b_j,a_j)$ and noting that $|\{w'\colon\ w' \xrightarrow{u} w\}| = |\{w'\colon\ w \xrightarrow{u'} w'\}|$. For the upper bound, select j sections with possible repeats in $\binom{M+j-1}{j}$ ways, to place the j lies of u in order. There are at most $(\frac{1}{t}\lceil Q/M\rceil + r + k)$ ways of applying lie (a_ℓ, b_ℓ) within its section, so that w yields w' as in (1). For the lower bound, use the bound $\frac{1}{t}\lceil Q/M\rceil - (t-1)r - 2 - k$ on the minimum letter frequency for w, or 0 if this quantity is negative, and then under-count by applying at most one lie per section. A C-shadow with stem w consists of all w' such that $w \stackrel{u}{\to} w'$ for some $u \in C$. Thus (8) follows by summing over u, graded by length $|u| = j$, and applying (7). □

We need the following lemma to handle applying lie strings to severely unbalanced vertices in the pathological (original) variant for Theorem 3.8 (3.9). In fact, this is the motivation for defining non-degenerate channels.

Lemma 3.6. *Let $Q \geqslant t(k-1)+1$, and let $w \in T^Q$. Let C be a channel of order k. If C is non-degenerate with respect to the original (pathological) variant, then $\bigcup_{u\in C}\{w'\colon w \stackrel{u}{\to} w'\}$ $(\bigcup_{u\in C}\{w'\colon w' \stackrel{u}{\to} w\})$ is non-empty.*

Proof. Since $Q \geqslant t(k-1)+1$, there exists a letter c with minimum frequency k in w. In the original (pathological) variant, let $a = c$ $(b = c)$. By Definition 2.2 there exists a $u \in C$ where $u = (a, b_1)\cdots(a, b_j)$ $(u = (a_1, b)\cdots(a_j, b))$ for $0 \leqslant j \leqslant k$. Construct w' with $w \stackrel{u}{\to} w'$ $(w' \stackrel{u}{\to} w)$ by applying u in j arbitrarily chosen positions in which w has a c. □

3.2. A packing within covering condition for Paul to win

We now characterize a winning condition in Theorem 3.7 for Paul at the transition to the second batch of questions, and go on to prove conditions for which Paul can win the whole game in both variants in Theorem 3.8. Paul's overall strategy in the original variant is to split $[n]$ into blocks of size α and assign a unique block address, chosen from balanced vertices in T^{q_1}, to each block. He forms his first batch of q_1 questions by inspecting each element's block address. Carole's first batch response w' yields a state vector $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$, following Definition 2.6. Paul's selection of balanced block addresses allows control on the entries of this state vector, i.e., which $y \in [n]$ survive and in what fashion, through Lemma 3.5. He then wins the second batch of q_2 questions, and thus the game (through the winning strategy/packing equivalence in Theorem 3.7), as follows. He constructs a packing in T^{q_2} of the C'-shadows corresponding to this state vector, fitting all but the singleton $\{\varepsilon\}$-shadows inside Hamming balls centered on balanced vertices of T^{q_2} in order to ensure separation and to control volume. The remaining empty space in T^{q_2} exceeds the number of these singletons, and so Paul can add singletons while preserving a packing, and his strategy is winning. Paul's strategy in the pathological variant piggy-backs his original variant strategy; he adds α' new elements to the above blocks of size α (thereby increasing n). This increases the entries of $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$ enough so that the original packing in T^{q_2} can be augmented by new singletons to form a covering. Unlike in the original variant, Paul must also handle the case in which Carole's first batch response w' is not close to being balanced. By assigning t^{q_2} new elements to each unbalanced block address in T^{q_1}, Paul guarantees by virtue of non-degeneracy of the channel having t^{q_2} singletons to cover T_{q_2}. In either case he wins by the winning strategy/covering equivalence in Theorem 3.7.

Theorem 3.7. *Let C be a channel, and let $(x_{C'}\colon C' \in \mathcal{S}(C))$ be the state vector at the beginning of a 1-batch, Q-round game on search space $[n]$. Then Paul can win the original (pathological) variant iff there exists an $(x_{C'}\colon C' \in \mathcal{S}(C))$-packing (-covering) of T^Q.*

Proof. Given Paul's strategy in either variant and an element $y \in [n]$ counted by $x_{C'(y)}$, let $w(y) = w_1 \cdots w_Q$ be the truthful response for y. For all i, y is in the w_ith part A_{w_i} of Paul's ith question. Then y survives the game iff Carole responds with $w' \in B(w(y), C'(y))$. Paul wins the original variant iff, for all responses w', at most one y survives, which occurs iff $\{B(w(y), C'(y))\}_{y\in[n]}$ is an $(x_{C'}\colon C' \in \mathcal{S}(C))$-packing in T^Q. Similarly, Paul wins the pathological variant iff for all responses w', at least one y survives, which occurs iff $\{B(w(y), C'(y))\}_{y\in[n]}$ is an $(x_{C'}\colon C' \in \mathcal{S}(C))$-covering of T^Q. □

Empty sets are allowed in either the packing or covering of Theorem 3.7. Paul's strategy determines the sets $B(w(y), C'(y))$, which might be empty when $C'(y)$ violates Definition 2.2 or Q is close to 0. Adding empty sets neither hurts a packing nor helps to form a covering. In the next theorem, the parameters M_1 and M_2 are the number of sections into which the first and second batches of q_1 and q_2 questions, respectively, are divided, according to Definition 3.1. This sectioning allows better counting of elements of $[n]$ with particular game lie strings by considering the sections in which lies occur. The parameters r_1 and r_2 provide an upper bound to the maximum letter frequency within sections in the first and second batches of questions, respectively; and η_1 and η_2 allow fine-tuning of r_1 and r_2 so that an appropriately large proportion of the strings of T^{q_1} and T^{q_2}, respectively, are balanced. Now we give the main conditions under which Paul has winning strategies.

Theorem 3.8. *Let C be a t-ary channel of order k, $q = q_1 + q_2$ be the number of rounds split into two positive integer batches, $\alpha, \alpha', M_1, M_2$ be positive integers, and let η_1, η_2 be positive reals. Following* (4)*, define $r_1 := r(q_1, M_1, \eta_1 \log_2 q)$ and $r_2 := r(q_2, M_2, \eta_2 \log_2 q)$. Let $c_k := (k^2 + 3k - 2)/2$, and define G and H as in* (6)*. If the packing condition*

$$\alpha \sum_{j=0}^{i} p_{k-i}^{(j)} G(q_1, M_1, r_1, j) \leqslant A_t\big(q_2 - c_k, 2(k-i)+1\big) - \frac{q^{-\eta_2} t^{q_2}}{b(q_2, t, k-i)} \tag{9}$$

holds for all $1 \leqslant k - i \leqslant k$, and the volume condition

$$\alpha \sum_{i=0}^{k} \sum_{j=0}^{i} E_i(C) G(q_1, M_1, r_1, j) G(q_2, M_2, r_2, i-j) \leqslant t^{q_2} \tag{10}$$

holds, then Paul can win the (n, q_1, q_2, C)-game when $n \leqslant \alpha(1 - q^{-\eta_1}) t^{q_1}$. Furthermore, if condition (9) *holds, C is non-degenerate with respect to the pathological variant, $q_1 \geqslant t(k-1)+1$, and in addition the volume condition*

$$\alpha \sum_{i=0}^{k} \sum_{j=0}^{i} E_i(C) H(q_1, M_1, r_1, j) H(q_2, M_2, r_2, i-j) + \alpha' \sum_{j=0}^{k} p_0^{(j)} H(q_1, M_1, r_1, j) \geqslant t^{q_2} \tag{11}$$

holds, then Paul can win the $(n, q_1, q_2, C)^*$-game when $n \geqslant (\alpha + \alpha')(1 - q^{-\eta_1}) t^{q_1} + t^q q^{-\eta_1}$.

Proof. For the original variant, Paul splits $[n]$ into blocks of size α and identifies in bijective correspondence each block with an (M_1, r_1)-balanced vertex of T^{q_1}. Paul's first q_1 questions ask for the q_1 digits of the distinguished element in this identification. By Lemma 2.7 and Theorem 3.7, Paul wins iff for any possible answer $w' \in T^{q_1}$ by Carole, yielding the game state vector $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$ of Definition 2.6, there exists an $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$-packing in T^{q_2}.

Claim 1. *If the packing condition* (9) *holds, then there exists an $(x_{C'}(w')\colon C' \in \mathcal{S}(C), o(C') \geqslant 1)$-packing in T^{q_2} with all stems in the set $\{z \in T^{q_2}\colon d(z, T^{q_2}(M_2, r_2)) \leqslant k\}$.*

Proof. Because every order $(k-i)$ shadow fits completely within a $(k-i)$-ball with the same center, it suffices to show there exists an $(x_i\colon 1 \leqslant k-i \leqslant k)$-packing in T^{q_2} with all centers in $\{z \in T^{q_2}\colon d(z, T^{q_2}(M_2, r_2)) \leqslant k\}$. Let $\mathcal{D}_{k-i} \subseteq T^{q_2 - c_k}$ be the set of centers of a size $A_t(q_2 - c_k, 2(k-i)+1)$ packing of $(k-i)$-balls. We construct an $(x_{k-i} = A_t(q_2 - c_k, 2(k-i)+1)\colon 1 \leqslant k-i \leqslant k)$-packing of Hamming balls in T^{q_2} as follows:

$$\begin{array}{rlllllll}
\mathcal{D}= & \underbrace{1\cdots1}_{k\ \text{times}} & 0\cdots0 & 0\cdots0 & \cdots & 00 & \mathcal{D}_k \\
\cup & 0\cdots0 & \underbrace{1\cdots1}_{k\ \text{times}} & 0\cdots0 & \cdots & 00 & \mathcal{D}_{k-1} \\
\cup & 0\cdots0 & 0\cdots0 & \underbrace{1\cdots1}_{k-1\ \text{times}} & \cdots & 00 & \mathcal{D}_{k-2} \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\cup & 0\cdots0 & 0\cdots0 & 0\cdots0 & \cdots & \underbrace{11}_{2\ \text{times}} & \mathcal{D}_1,
\end{array}$$

in which the centers of the $(k-i)$-balls in $\mathcal{D}$ are taken to be the extensions of their original centers in $\mathcal{D}_{k-i}$. By construction, two distinct balls of radius i and j are disjoint, as the distance between their centers is at least $i+j+1$. By Lemma 3.2, for fixed $k-i$, the number of $(k-i)$-balls in the packing $\mathcal{D}$ comprised entirely of (M_2,r_2)-unbalanced vertices is at most $q^{-\eta_2}t^{q_2}/b(q_2,t,k-i)$. After deleting the corresponding centers from $\mathcal{D}$, at least $A_t(q_2-c_k,2(k-i)+1)-q^{-\eta_2}t^{q_2}/b(q_2,t,k-i)$ $(k-i)$-balls with centers in $\{z\in T^{q_2}\colon\ d(z,T^{q_2}(M_2,r_2))\leqslant k\}$ remain. We finish the claim by showing that for any response w' by Carole, the left-hand side of (9) is an upper bound on x_i for $1\leqslant k-i\leqslant k$:

$$x_i=\sum_{\substack{C'\in\mathcal{S}(C)\\ o(C')=k-i}}x_{C'}\leqslant\alpha\sum_{\substack{C'\in\mathcal{S}(C)\\ o(C')=k-i}}\ \sum_{u,\,S_C(u)=C'}\bigl|\{w\colon\ w\overset{u}{\to}w'\}\bigr| \tag{12}$$

$$=\alpha\sum_{j=0}^{i}\ \sum_{\substack{u,\,|u|=j\\ o(S_C(u))=k-i}}\bigl|\{w\colon\ w\overset{u}{\to}w'\}\bigr|\leqslant\alpha\sum_{j=0}^{i}p_{k-i}^{(j)}G(q_1,M_1,r_1,j). \tag{13}$$

Line (12) is by the definitions of x_i, $x_{C'}$, and $w\overset{u}{\to}w'$, where the inequality is because the unbalanced w contribute nothing to $x_{C'}$. The equality in (13) is by a straightforward reindexing of the summation. The inequality in (13) is by the definition of $p_{k-i}^{(j)}$ and Lemma 3.5 since Carole's response w' must satisfy $d(w',T^{q_1}(M_1,r_1))\leqslant k$, or else she defaults as all elements of $[n]$ are identified with (M_1,r_1)-balanced strings. □

Claim 2. *If the packing condition* (9) *and the volume condition* (10) *both hold, then there exists an* $(x_{C'}(w')\colon\ C'\in\mathcal{S}(C))$*-packing in* T^{q_2}.

Proof. To show that such a packing exists, it is enough to demonstrate that x_k 0-balls (singletons) can be packed in the unoccupied space of the packing in Claim 1. We therefore show that the total volume of the packing in Claim 1 and the singletons is at most the left-hand side of (10). For $0\leqslant i<k$, every $S_C(u)$-shadow in the packing in T^{q_2} counted by (13) is bounded in size by Lemma 3.5, because all stems of the packing in Claim 1 are in $\{z\in T^{q_2}\colon\ d(z,T^{q_2}(M_2,r_2))\leqslant k\}$. Hence the space occupied by the packing from Claim 1 is

$$\leqslant\alpha\sum_{i=0}^{k}\sum_{j=0}^{i}\ \sum_{\substack{u,\,|u|=j\\ o(S_C(u))=k-i}}\bigl|\{w\colon\ w\overset{u}{\to}w'\}\bigr|\ \max_{\substack{z\in T^{q_2}\\ d(z,T^{q_2}(M_2,r_2))\leqslant k}}\bigl|B\bigl(z,S_C(u)\bigr)\bigr|. \tag{14}$$

The singletons, counted when $i=k$, are all volume 1 $\{\epsilon\}$-shadows with $B(z,\{\epsilon\})=\{z\}$ regardless of z. Applying Lemma 3.5, (14) is

$$\leqslant\alpha\sum_{i=0}^{k}\sum_{j=0}^{i}\ \sum_{\substack{u,\,|u|=j\\ o(S_C(u))=k-i}}G(q_1,M_1,r_1,j)\sum_{\ell=0}^{k-i}\ \sum_{\substack{v\in S_C(u)\\ |v|=\ell}}G(q_2,M_2,r_2,\ell) \tag{15}$$

$$= \alpha \sum_{i=0}^{k} \sum_{j+\ell \leqslant k} \sum_{\substack{uv \in E_{j+\ell}(C) \\ o(S_C(u))=k-i \\ |u|=j,\, |v|=\ell}} G(q_1, M_1, r_1, j) G(q_2, M_2, r_2, \ell) \tag{16}$$

$$= \alpha \sum_{j+\ell \leqslant k} \sum_{\substack{uv \in E_{j+\ell}(C) \\ |u|=j,\, |v|=\ell}} G(q_1, M_1, r_1, j) G(q_2, M_2, r_2, \ell) \tag{17}$$

$$= \alpha \sum_{i=0}^{k} \sum_{j=0}^{i} E_i(C) G(q_1, M_1, r_1, j) G(q_2, M_2, r_2, i-j). \tag{18}$$

The double sums over j and ℓ combine to a sum over $j+\ell \leqslant k$ in (16) because, for $j > i$, there are no u with $|u| = j$ and $o(S_C(u)) = (k-i)$. By interchanging the first two summations in (16), the sum over i has the effect of summing over the orders of $S_C(u)$, and since each $u \in C$ has a unique $o(S_C(u))$, we have (17). Finally, setting $j + \ell = i$ gives (18), completing the proof of Claim 2. □

Therefore Paul wins if n is α times the number of (M_1, r_1)-balanced vertices in T^{q_1}, which is at least $(1 - q^{-\eta_1})t^{q_1}$ by Lemma 3.2. If n is less than this number, Paul can clearly still win by simply removing shadows from the packing.

For the pathological variant, Paul identifies $(\alpha + \alpha')$ elements of $[n]$ with each of the (M_1, r_1)-balanced vertices of T^{q_1}, and t^{q_2} elements with each (M_1, r_1)-unbalanced vertex. We may assume $\alpha \leqslant \alpha + \alpha' < t^{q_2}$, for suppose to the contrary $\alpha + \alpha' \geqslant t^{q_2}$. Then Paul can win by the following argument. Let w' be Carole's response after the first batch of questions. By Lemma 3.6, there exist $u \in C$ and $w \in T^{q_1}$ with $\{w \xrightarrow{u} w'\}$. There are at least t^{q_2} elements identified with w that will survive the first batch with suffix channel $C' = S_C(u)$ containing ϵ. In the second batch, Paul identifies at least one of these elements counted by $x_{C'}$ to each vertex of T^{q_2} and asks for the q_2 digits of the distinguished element. Regardless of Carole's response $z' \in T^{q_2}$, the element(s) identified with z' survives.

As in the original variant, Paul's first q_1 questions ask for the q_1 digits of the distinguished element in the above identification. By Theorem 3.7, Paul wins iff for all possible answers $w' \in T^{q_1}$ by Carole, yielding the game state vector $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$ of Definition 2.6, there exists an $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$-covering of T^{q_2}.

Claim 3. *If the packing condition* (9) *holds, C is non-degenerate with respect to the pathological variant, $q_1 \geqslant t(k-1)+1$, and the volume condition* (11) *holds, then there exists an $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$-covering of T^{q_2}.*

Proof. We first consider the case in which $d(w', T^{q_1}(M_1, r_1)) \leqslant k$. For this case, consider only $\alpha + \alpha'$ elements of $[n]$ identified per $w \in T^{q_1}$. The state vector $(x_{C'}(w')\colon C' \in \mathcal{S}(C))$ can be split into $(x_{C'}(w')|_{\alpha}\colon C' \in \mathcal{S}(C))$ and $(x_{C'}(w')|_{\alpha'}\colon C' \in \mathcal{S}(C))$ from the contributions of α and α', respectively. By (9) and Claim 1, there exists an $(x_{C'}(w')|_{\alpha}\colon C' \in \mathcal{S}(C), o(C') \geqslant 1)$-packing in T^{q_2}, with all stems in the set $\{z \in T^{q_2}\colon d(z, T^{q_2}(M_2, r_2)) \leqslant k\}$. If the volume after adding in the α elements identified with each singleton is $> t^{q_2}$ we have a covering, and we are done. Otherwise, we have an $(x_{C'}(w')|_{\alpha}\colon C' \in \mathcal{S}(C))$-packing in T^{q_2}.

Considering only the first α elements identified with each vertex of T^{q_1}, Eq. (12) becomes equality throughout, and the volume of the $(x_{C'}(w')|_{\alpha}\colon C' \in \mathcal{S}(C))$-packing (analogous to (14)) is

$$\geqslant \sum_{i=0}^{k} \sum_{j=0}^{i} \sum_{\substack{u,\, |u|=j \\ o(S_C(u))=k-i}} \alpha \left|\{w\colon w \xrightarrow{u} w'\}\right| \min_{\substack{z \in T^{q_2} \\ d(z, T^{q_2}(M_2, r_2)) \leqslant k}} \left|B\big(z, S_C(u)\big)\right|. \tag{19}$$

The singletons, counted when $i = k$, are all volume 1 $\{\epsilon\}$-shadows with $B(z, \{\epsilon\}) = \{z\}$ regardless of z. Applying Lemma 3.5, and manipulating the summations as in (15)–(18), (19) is

$$\geqslant \alpha \sum_{i=0}^{k} \sum_{j=0}^{i} E_i(C) H(q_1, M_1, r_1, j) H(q_2, M_2, r_2, i - j). \tag{20}$$

Following (12), the additional α' elements identified with each vertex of T^{q_1} have a contribution to $x_{\{\epsilon\}}$ of exactly

$$x_{\{\epsilon\}}|_{\alpha'} = \sum_{u,\, S_C(u)=\{\epsilon\}} \alpha' \left| \{w\colon\ w \stackrel{u}{\to} w'\} \right| \geqslant \sum_{j=0}^{k} \sum_{\substack{u,\, |u|=i \\ S_C(u)=\{\epsilon\}}} \alpha' H(q_1, M_1, r_1, j)$$
$$= \alpha' \sum_{j=0}^{k} p_0^{(j)} H(q_1, M_1, r_1, j)$$

which by volume condition (11) and (20) is at least the number of vertices of T^{q_2} not covered in the $(x_{C'}(w')|_\alpha\colon\ C' \in \mathcal{S}(C))$-packing. We extend to an $(x_{C'}(w')\colon\ C' \in \mathcal{S}(C))$-covering of T^{q_2} by using at most $x_{\{\epsilon\}}|_{\alpha'}$ $\{\epsilon\}$-shadows to cover, with $B(z, \{\epsilon\})$, any $z \in T^{q_2}$ not covered by the packing. Based on the covering constraint, any unaccounted-for shadows in the original identification of elements of $[n]$ to vertices of T^{q_1} may be ignored.

Now assume that Carole responds to the first q_1 questions with $w' \in T^{q_1}$ and $d(w', T^{q_1}(M_1, r_1)) > k$. Again, let $(x_{C'}(w')\colon\ C' \in \mathcal{S}(C))$ be the state vector after Carole's response. By Lemma 3.6, there exists a $u \in C$ and a $w \in T^{q_1}$ such that $w \stackrel{u}{\to} w'$. Since $|u| \leqslant k$, $d(w', w) \leqslant k$, and so w is (M_1, r_1)-unbalanced. Thus the t^{q_2} elements identified with w have suffix channel $S_C(u)$ containing ϵ, so that $x_{S_C(u)} \geqslant t^{q_2}$. The collection of $S_C(u)$-shadows $\{B(z, S_C(u))\colon\ z \in T^{q_2}\}$ covers T^{q_2}, since $\epsilon \in S_C(u)$ implies $z \in B(z, S_C(u))$. There exists an $(x_{C'}(w')\colon\ C' \in \mathcal{S}(C))$-covering of T^{q_2} by placing the remaining shadows arbitrarily. □

Therefore, whether w' is close to being balanced or not, Paul wins with n equal to $(\alpha + \alpha')$ times the number of (M_1, r_1)-balanced vertices of T^{q_1} and t^{q_2} times the number of (M_1, r_1)-unbalanced vertices of T^{q_1}. By Lemma 3.2, this is at most $(\alpha + \alpha')(1 - q^{-\eta_1})t^{q_1} + t^q q^{-\eta_1}$. Paul can win for any $n' > n$ by treating extra elements arbitrarily without disturbing the covering constructed above. □

3.3. A condition for Carole to win

The following theorem gives conditions under which Carole has winning strategies in both the original and pathological 2-batch games, by way of non-existence of packings or coverings, respectively, corresponding to winning strategies for Paul.

Theorem 3.9. *Let C be a t-ary channel of order k, $q = q_1 + q_2$ be the number of rounds split into two positive integer batches, M_1, M_2 be positive integers, and let η_1, η_2, η be positive reals. Following* (4)*, define $r_1 := r(q_1, M_1, \eta_1 \log_2 q)$, $r_2 := r(q_2, M_2, \eta_2 \log_2 q)$, and $r := r(q, M, \eta \log_2 q)$; define G and H as in* (6)*. If C is non-degenerate with respect to the original variant, $q_1, q_2 \geqslant t(k-1) + 1$, and, in addition, the volume condition*

$$n > t^q \bigl(E_k(C)\bigl(H(q_1, M_1, r_1, k) + H(q_2, M_2, r_2, k)\bigr)\bigr)^{-1} + \bigl(q^{-\eta_1} + q^{-\eta_2}\bigr) t^q \tag{21}$$

holds, then Carole can win the (n, q_1, q_2, C)-game. If the volume condition

$$n < t^q \bigl(1 - q^{-\eta}\bigr) \left(\sum_{i=0}^{k} E_i(C) \binom{M + i - 1}{i} \left(\frac{1}{t} \left\lceil \frac{q}{M} \right\rceil + r + 1 \right)^i \right)^{-1} \tag{22}$$

holds, then Carole can win the $(n, q_1, q_2, C)^*$-game.

Proof. We define the *response set* of an element y of the search space $[n]$ to be $\mathcal{R}(y) := \{w'z' \in T^q\colon$ y survives with game response string $w'z'\}$. Call a response string $w'z'$ *doubly balanced* if $w' \in T^{q_1}$ is (M_1, r_1)-balanced, and $z' \in T^{q_2}$ is (M_2, r_2)-balanced. We say y is *typical* if every $w'z' \in \mathcal{R}(y)$ is doubly balanced.

For the original variant, Carole can win if $\{\mathcal{R}(y)\colon\ y \in [n]\}$ is not a packing, since if $\mathcal{R}(y) \cap \mathcal{R}(y') \neq \emptyset$, then there exists a $w'z'$ for which both y and y' survive. Assume y is typical. Let $w = w(y)$ be the truthful first batch response for y. We may assume $d(w, T^{q_1}(M_1, r_1)) \leqslant k$. Otherwise, since C is non-degenerate, by Lemma 3.6 there exists a $u \in C$ such that $w \xrightarrow{u} w'$ with w' (M_1, r_1)-unbalanced, making y atypical.

We under-count $\mathcal{R}(y)$ by counting only those w' with $w \xrightarrow{u} w'$ for $u = \epsilon$ or $u \in C$ with $|u| = k$, thus guaranteeing that $S_C(u)$ is non-degenerate. Using Lemma 3.5, the number of such w' is at least $1 + E_k(C)H(q_1, M_1, r_1, k)$, where the 1 term corresponds to $u = \epsilon$. If y survives the first batch given that Carole's response is one of these w', then Paul's strategy determines the truthful z for y in the second batch. As before, z must satisfy $d(z, T^{q_2}(M_2, r_2)) \leqslant k$, or else y survives for an unbalanced z'. The number of z' for which y survives the second batch is dependent on the suffix channel $S_C(u)$, and is at least $E_k(C)H(q_2, M_2, r_2, k)$ when $u = \epsilon$ and 1 otherwise. Therefore, similar to (15)–(18) (with many terms omitted), the size of $\mathcal{R}(y)$ is at least

$$E_k(C)\big(H(q_1, M_1, r_1, k) + H(q_2, M_2, r_2, k)\big).$$

If y is atypical, then there exists a response sequence $w'z'$ for which y survives, and either w' is (M_1, r_1)-unbalanced, or z' is (M_2, r_2)-unbalanced. Thus there is at least one non-doubly balanced string in $\mathcal{R}(y)$. By Lemma 3.2, there are at most $(q^{-\eta_1} + q^{-\eta_2})t^q$ such $w'z'$.

We can pack at most $t^q(E_k(C)(H(q_1, M_1, r_1, k) + H(q_2, M_2, r_2, k)))^{-1}$ response sets for y typical and, independently, at most $(q^{-\eta_1} + q^{-\eta_2})t^q$ response sets for y atypical. Therefore, if (21) holds, Carole can win.

For the pathological variant, Carole can win if $\{\mathcal{R}(y)\colon\ y \in [n]\}$ is not a covering, since for $w \in T^q$, if $w' \notin \bigcup_{y\in[n]} \mathcal{R}(y)$, then w' is a response for which no element y survives. We further handicap Carole by allowing Paul full adaptivity, i.e., Paul can wait to ask each question until after Carole responds to the previous question. If Carole can win the fully adaptive case, she can certainly win the two-batch case for any q_1 and q_2.

We bound the number of (M, r)-balanced strings in $\mathcal{R}(y)$ for arbitrary $y \in [n]$. Each balanced string in $\mathcal{R}(y)$ is a result of applying a length i lie string, $0 \leqslant i \leqslant k$, to the truthful sequence of responses to Paul's queries, and is therefore identified by the lie string and positions of the lies. Divide Carole's q responses into M blocks as in Definition 3.1. Carole selects $u \in C$ with $|u| = i$ in $E_i(C)$ ways, and the i sections in which to place the lies of u in order in $\binom{M+i-1}{i}$ ways.

The first lie (a, b) of u to be placed in any block must occur within the first $(\frac{1}{t}\lceil\frac{q}{M}\rceil + r + 1)$ occurrences of a in that block; otherwise all of the resulting game response strings will be unbalanced. This restriction holds for every subsequent lie; therefore the maximum number of balanced strings in $\mathcal{R}(y)$ is at most

$$\sum_{i=0}^{k} E_i(C)\binom{M+i-1}{i}\left(\frac{1}{t}\left\lceil\frac{q}{M}\right\rceil + r + 1\right)^i.$$

By Lemma 3.2, there are at least $t^q(1 - q^{-\eta})$ (M, r)-balanced strings in t^q. Thus at least $t^q(1 - q^{-\eta})\big(\sum_{i=0}^{k} E_i(C)\binom{M+i-1}{i}(\frac{1}{t}\lceil\frac{q}{M}\rceil + r + 1)^i\big)^{-1}$ response sets are necessary to cover t^q. Therefore, if (22) holds, Carole can win. □

3.4. *An asymptotic approximation and Varshamov bound for the main theorem*

In order to convert Theorems 3.8–3.9 to asymptotic form, we require the technical Lemma 3.10 and an asymptotic form of a generalized Varshamov bound in Corollary 3.13. Lemma 3.10 will be used several times to approximate quantities such as G and H of (6). An asymptotic version of the packing condition (9) is allowed by bounding $A_t(Q, 2R + 1)$ with Theorem 3.11, when t is a prime power, generalizing to t not a prime power with Lemma 3.12, and converting to asymptotic form with Corollary 3.13.

Lemma 3.10. *Let $\ell \in \mathbb{Z}$, $j \in \mathbb{Z}_{\geqslant 0}$, $c_7, c_8 \in \mathbb{R}$, and $\eta \in \mathbb{R}^+$ be constants. Let $q \to \infty$, and let $f(q)$ be nonnegative with $f(q) \to \infty$. Let Q satisfy $(\ln q)^{3/2} f(q) \leqslant Q \leqslant q$. Let $M = \lceil Q^{1/3} \rceil$. Then*

$$\binom{M+\ell}{j}\left(\frac{1}{t}\left\lceil \frac{Q}{M}\right\rceil + c_7\sqrt{\left\lceil \frac{Q}{M}\right\rceil \frac{\ln(tMq^{\eta})}{2}} + c_8\right)^j$$
$$= \binom{Q}{j} t^{-j}\left(1 + \frac{tjc_7}{\sqrt{2}}\frac{\sqrt{\ln(Q^{1/3}q^{\eta})}}{Q^{1/3}}\big(1+o(1)\big)\right). \tag{23}$$

Proof. First, note that for any $N \to \infty$,

$$\binom{N+\ell}{j} = \frac{N^j}{j!}\left(1 \pm \Theta\left(\frac{1}{N}\right)\right). \tag{24}$$

Applying (24) to $\binom{M+\ell}{j}$ and replacing $\lceil Q/M \rceil$ with $Q/M + \Theta(1)$, the left-hand side of (23) becomes

$$= \frac{M^j}{j!}\left(1 \pm \Theta\left(\frac{1}{M}\right)\right)\left(\frac{Q}{tM} + c_7\sqrt{\left(\frac{Q}{M} + O(1)\right)\frac{\ln(tMq^{\eta})}{2}} \pm O(1)\right)^j.$$

Factoring out $(Q/(tM))^j$ from the last factor, and expanding the square root and the entire last factor using $(1+x)^p = 1 + px + O(x^2)$ as $x \to 0$, this becomes

$$= \frac{M^j}{j!}\frac{Q^j}{t^j M^j}\left(1 \pm \Theta\left(\frac{1}{M}\right)\right)\left(1 + tjc_7\sqrt{\frac{M}{Q}\frac{\ln(tMq^{\eta})}{2}} + O\left(\frac{M}{Q}\ln q\right)\right).$$

Applying (24) to $Q^j/j!$, noting that $\ln(t) = o(\ln(q))$ and $M = Q^{1/3} + O(1)$, and applying the binomial expansion on the square root again, this becomes the right-hand side of (23). The constraint $Q \geqslant (\ln q)^{3/2} f(q)$ allows collection of lower order terms into the $(1 + o(1))$ factor. □

The Varshamov lower bound for $A_t(Q, 2R+1)$, for t a prime power, relies on a construction on a vector space over a finite field, and can be found, for example, as Theorem 3.4 of [12]. A *linear code* with minimum distance $2R+1$ may be viewed as a packing of R-balls whose centers form a vector space.

Theorem 3.11 *(Varshamov bound). Let $t \geqslant 2$ be a prime power, and let $Q \geqslant 1$ and $R \geqslant 0$ be integers. Then*

$$A_t(Q, 2R+1) \geqslant B_t(Q, 2R+1) \geqslant t^{Q - \lceil \log_t(1 + \sum_{i=0}^{2R-1}\binom{Q-1}{i}(t-1)^i)\rceil},$$

where $B_t(Q, 2R+1)$ is the maximum size of a linear code of length Q, alphabet t, and minimum distance $2R+1$.

The following lemma allows extension to a weakened version of the Varshamov bound for t not a prime power. The lemma is due to Gevorkyan [13], but can also be found within the proof of Lemma 2 of [14]. We include the proof here for clarity.

Lemma 3.12. *Let $t_2 \geqslant t_1 \geqslant 2$, $Q \geqslant 1$ and $R \geqslant 0$ be integers. Then*

$$A_{t_1}(Q, 2R+1) \geqslant (t_1/t_2)^Q A_{t_2}(Q, 2R+1).$$

Proof. Define $T_1 := \{0, \dots, t_1 - 1\}$ and $T_2 := \{0, \dots, t_2 - 1\}$. Let $\mathcal{V}_2 \subseteq T_2^Q$ be the set of strings which are the centers of R-balls in a packing of T_2^Q. In particular, assume $|\mathcal{V}_2| = A_{t_2}(Q, 2R+1)$. View the strings of $\mathcal{V}_2 \subseteq T_2^Q$ as elements of the additive group $\mathbb{Z}_{t_2}^Q$. Let $w \in T_2^Q$, and define the translation $\mathcal{V}_2^w := \{w + w'\colon\ w' \in \mathcal{V}_2\}$ of $\mathcal{V}_2$. Let $z \in \mathbb{Z}_{t_1}^Q$ be viewed as an element of $\mathbb{Z}_{t_2}^Q$ since $t_1 \leqslant t_2$. Since $\mathbb{Z}_{t_2}^Q$ is a group, the number of translations of $\mathcal{V}_2$ containing z is $|\{w\colon\ z \in \mathcal{V}_2^w\}| = |\mathcal{V}_2|$. The average number of elements of $\mathbb{Z}_{t_1}^Q$ contained in a translate $\mathcal{V}_2^w$ is thus $|\mathbb{Z}_{t_1}^Q| \cdot |\mathcal{V}_2| / |\mathbb{Z}_{t_2}^Q| = (t_1/t_2)^Q |\mathcal{V}_2|$, and there must exist a translate $\mathcal{V}_2^{w^*}$ with at least this average. Translation preserves distance between strings, and so we may take the centers of the R-balls in our packing of T_1^Q to be $\mathcal{V}_2^{w^*} \cap T_1^Q$. $\square$

Corollary 3.13. *Let $t \geqslant 2$, $Q \geqslant 1$ and $k \geqslant R \geqslant 0$ be integers. Let $c_k = (k^2 + 3k - 2)/2$ as in Theorem* 3.8, *and let $c_9 < 1$ be an arbitrary constant. Then with t and R fixed, for Q large enough,*

$$A_t(Q - c_k, 2R+1) > c_9 \frac{(2R-1)!}{2^{2R}(t-1)^{2R-1}} \frac{t^{Q-c_k-1}}{Q^{2R-1}}.$$

Proof. Set $t_1 = t$, and let t_2 be the smallest prime power for which $t_1 \leqslant t_2$. In particular, $t_2 \leqslant 2t_1 - 1$. Applying Lemma 3.12 and Theorem 3.11, we have

$$\begin{aligned} A_{t_1}(Q - c_k, 2R+1) &\geqslant t_1^{Q-c_k} t_2^{-\lceil \log_{t_2}(1 + \sum_{i=0}^{2R-1} \binom{Q-c_k-1}{i}(t_2-1)^i) \rceil} \\ &\geqslant \frac{t_1^{Q-c_k} t_2^{-1}}{1 + \sum_{i=0}^{2R-1} \binom{Q-c_k-1}{i}(t_2-1)^i} > \frac{1}{2} \frac{t^{Q-c_k-1}}{1 + \sum_{i=0}^{2R-1} \binom{Q-c_k-1}{i} 2^i (t-1)^i}, \end{aligned}$$

from which the result follows by observing that the denominator is dominated by the $i = 2R - 1$ term. $\square$

3.5. *Proofs of the main result: Winning conditions for Paul and Carole*

We now apply the results of Section 3.4 and standard asymptotic analysis to prove Theorems 2.3–2.4.

Proof of Theorem 2.3. Let $c_2 > c_{10} > tk(k+1)\sqrt{k+2}/\sqrt{2}$ be constants and let

$$\alpha = \left\lfloor \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \left(1 - c_{10} \frac{\sqrt{\ln q}}{q_2^{1/3}}\right) \right\rfloor.$$

Fix $M_1 = \lceil q_1^{1/3} \rceil$ and $M_2 = \lceil q_2^{1/3} \rceil$. Let $\eta_1 = \eta_2 = k + 1$. Let $c_1 < c_{11} < (\frac{(2k-1)! t^{-c_k-k-1} E_k(\mathcal{C})}{2^{2k}(t-1)^{2k-1} k!})^{1/(2k-1)}$ be constants, and let $c_{12} > 1$ and $c_9 < 1$ be constants such that $c_1 < (c_9/c_{12})^{1/(2k-1)} c_{11}$. Applying Lemma 3.10 and (24), and noting that the terms for $0 \leqslant j < i$ are asymptotically negligible, for q (and thus q_1) sufficiently large, the left-hand side of (9) is

$$< c_{12} \frac{t^{q_2+k} k!}{E_k(C) q^k} \frac{p_{k-i}^{(i)}}{t^i} \frac{q_1^i}{i!}. \tag{25}$$

Applying Corollary 3.13 and (5), for q (and thus q_2) sufficiently large, the right-hand side of (9) is

$$A_t\bigl(q_2 - c_k, 2(k-i)+1\bigr) - \frac{q^{-k-1} t^{q_2}}{b(q_2, t, k-i)} > c_9 \frac{(2(k-i)-1)!}{2^{2(k-i)}(t-1)^{2(k-i)-1}} \frac{t^{q_2-c_k-1}}{q_2^{2(k-i)-1}}, \tag{26}$$

since the assumption $1 \leqslant k - i \leqslant k$ for (9) makes $q^{-k-1} t^{q_2} / b(q_2, t, k-i)$ asymptotically negligible. For (9) to hold, it will suffice that (25) be at most the right-hand side of (26), for $1 \leqslant k - i \leqslant k$. This is immediate when $p_{k-i}^{(i)} = 0$; otherwise the condition is equivalent to

$$q_2^{2(k-i)-1} \leqslant \frac{c_9}{c_{12}} \frac{(2(k-i)-1)! t^{-c_k-(k-i)-1} E_k(C) i!}{2^{2(k-i)}(t-1)^{2(k-i)-1} p_{k-i}^{(i)} k!} \frac{q^k}{q_1^i}. \tag{27}$$

The restrictive case is $k-i=k$; if $q_2 \leqslant c_1 q^{k/(2k-1)}$, then for q large enough, (27) and thus (9) holds for all $1 \leqslant k-i \leqslant k$.

Applying Lemma 3.10 and noting that $q_2 = o(q_1)$, the left-hand side of the volume condition (10) is equal to

$$\alpha \sum_{i=0}^{k} \sum_{j=0}^{i} E_i(C) \frac{\binom{q_1}{j}\binom{q_2}{i-j}}{t^i} \left(1 + \frac{t(i-j)}{\sqrt{2}} \frac{\sqrt{\ln(q_2^{1/3} q^{k+1})}}{q_2^{1/3}} \bigl(1+o(1)\bigr)\right). \tag{28}$$

Using the identity $\sum_{j=0}^{i} \binom{q_1}{j}\binom{q_2}{i-j} = \binom{q}{i}$, noting that all terms $i<k$ are negligible, bounding $t(i-j) \leqslant tk$, and bounding $\ln(q_2^{1/3} q^{k+1}) \leqslant (k+2)\ln q$, (28) is

$$\leqslant \alpha E_k(C) \frac{\binom{q}{k}}{t^k} \left(1 + \frac{tk(k+1)\sqrt{k+2}}{\sqrt{2}} \frac{\sqrt{\ln q}}{q_2^{1/3}} \bigl(1+o(1)\bigr)\right) = t^{q_2}\bigl(1-o(1)\bigr). \tag{29}$$

By the choice of α, (10) holds for q large enough, so that by Theorem 3.8 Paul can win the (n, q_1, q_2, C)-game for

$$n \leqslant \alpha\bigl(1-q^{-\eta_1}\bigr)t^{q_1} = \left\lfloor \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \left(1 - c_{10} \frac{\sqrt{\ln q}}{q_2^{1/3}}\right) \right\rfloor \bigl(1-q^{-k-1}\bigr)t^{q_1},$$

where for q large enough, this last quantity is at least the right-hand side of (2).

For the pathological variant, let $c_{13} > t^2 k(k+1)\sqrt{k+2}/\sqrt{2}$ and $c_3 > t(t-1)k(k+1)\sqrt{k+2}/\sqrt{2}$ be constants such that $c_{13} - t(t-1)k(k+1)\sqrt{k+2}/\sqrt{2} > c_{10}$, and $c_3 > c_{13} - c_{10}$. Let

$$\alpha' = \left\lceil c_{13} \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \frac{\sqrt{\ln(q)}}{q_2^{1/3}} \right\rceil.$$

Following the derivation of (25) and (29), for q sufficiently large, the left-hand side of the volume condition (11) is

$$\geqslant \left\lfloor \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \left(1 - c_{10}\frac{\sqrt{\ln q}}{q_2^{1/3}}\right) \right\rfloor E_k(C) \frac{\binom{q}{k}}{t^k} \left(1 - \frac{t(t-1)k(k+1)\sqrt{k+2}}{\sqrt{2}} \frac{\sqrt{\ln(q)}}{q_2^{1/3}} \bigl(1+o(1)\bigr)\right)$$
$$+ \left\lceil c_{13} \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \frac{\sqrt{\ln(q)}}{q_2^{1/3}} \right\rceil E_k(C) \frac{\binom{q}{k}}{t^k} \bigl(1-o(1)\bigr) \geqslant t^{q_2},$$

by definition of α', c_{13}, and c_{10}. Therefore for q sufficiently large, by Theorem 3.8, Paul can win the $(n, q_1, q_2, C)^*$-game for

$$n \geqslant \bigl(\alpha+\alpha'\bigr)\bigl(1-q^{-\eta_1}\bigr)t^{q_1} + t^q q^{-\eta_1}$$
$$= \left(\left\lfloor \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \left(1 - c_{10}\frac{\sqrt{\ln q}}{q_2^{1/3}}\right) \right\rfloor + \left\lceil c_{13} \frac{t^{q_2+k}}{E_k(C)\binom{q}{k}} \frac{\sqrt{\ln(q)}}{q_2^{1/3}} \right\rceil\right) \bigl(1-q^{-k-1}\bigr)t^{q_1} + t^q q^{-k-1}.$$

By definition of c_3, for q sufficiently large, this last quantity is at most the right-hand side of (3). □

Proof of Theorem 2.4. Fix $\eta_1 = \eta_2 = \eta = k+1$, and define $c_{14} := t(t-1)k\sqrt{k+2}/\sqrt{2}$. By applying Lemma 3.10, and noting that $\ln(q_1^{1/3} q^{\eta_1}), \ln(q_2^{1/3} q^{\eta_2}) \leqslant (k+2)\ln q$, the right-hand side of (21) is

$$\leqslant t^q \left(\frac{E_k(C)}{t^k} \left(\binom{q_1}{k} \left(1 - c_{14} \frac{\sqrt{\ln q}}{q_1^{1/3}} \bigl(1+o(1)\bigr)\right) + \binom{q_2}{k} \left(1 - c_{14} \frac{\sqrt{\ln q}}{q_2^{1/3}} \bigl(1+o(1)\bigr)\right)\right)\right)^{-1} + 2q^{-k-1}t^q. \tag{30}$$

In asymptotically achieving the sphere bound, we cannot have $\min(q_1, q_2)$ too large, since (for example)

$$\binom{q_2}{k} = \binom{q}{k}\left(\frac{q_2}{q}\right)^k\left(1 - \frac{q_1}{q_2}\frac{k(k-1)}{2q}\big(1-o(1)\big)\right).$$

Assuming for convenience that $q_2 = \min(q_1, q_2)$, since $2q^{-k-1}t^q$ is asymptotically negligible, the right-hand side of (30) becomes

$$t^q\left(\frac{E_k(C)}{t^k}\binom{q}{k}\left(1 - \left(\frac{kq_2}{q} + \frac{c_{14}\sqrt{\ln q}}{q_1^{1/3}} - \left(\frac{q_2}{q}\right)^k\right)\big(1+o(1)\big)\right)\right)^{-1}.$$

The result for the original variant follows by selecting any $c_4 > k$ (or $c_4 > 0$ when $k = 1$) and $c_5 > c_{14}$ and applying Theorem 3.9. For the pathological variant, the $i = k$ term dominates the right-hand side of (22), which is asymptotically

$$= t^q\big(1 - q^{-k-1}\big)\left(\frac{E_k(C)}{t^k}\binom{q}{k}\left(1 + \frac{tk\sqrt{k+2}}{\sqrt{2}}\frac{\sqrt{\ln q}}{q^{1/3}}\big(1+o(1)\big)\right)\right)^{-1}.$$

The result follows by selecting any $c_6 > tk\sqrt{(k+2)/2}$, noting that $(1 - q^{-k-1})$ is asymptotically negligible, and applying Theorem 3.9. □

4. Concluding remarks

The first asymptotic term of Theorems 2.3–2.4 is the *sphere bound* for liar games (adaptive codes) over C. It arises by counting the expected number of game response strings for which $y \in [n]$ survives when Paul's partitions are random, and dividing into the size of the space T^q. Paul's embedding strategy in Theorem 3.8 can be viewed as a quasirandom implementation of this notion.

The most important consequence of Theorem 2.3, in the language of coding theory, is the existence of asymptotically perfect adaptive codes for a wide range of parameters when the total number of errors (lies) is bounded. The dominating asymptotic term depends only on the number of lie strings of maximum length in C and not on their shape.

The generality of the channel led us to make trade-offs for clarity's sake. For example, the second asymptotic term in (2)–(3) could be reduced to $O(q_2^{-1/3})$ by a more careful embedding of $[n]$ in T^{q_1}, and to $O(q_2^{-1/2})$ by assuming that C is closed under reordering of lie strings. When $t = 2$, the so-called BCH codes [12] provide a superior bound for $A_t(Q, 2R+1)$, allowing the second batch size to be increased to $q_2 = \Theta(q)$ without disturbing the form of the result. When the suffix channel $S_C(u')$ of every prefix u' of a length k lie string u in C is non-degenerate, the original variant bound in Theorem 2.4 improves to $n \geqslant t^{q+k}(E_k(C)\binom{q}{k})^{-1}(1 + \text{const.} \cdot \sqrt{\ln q}(1/q_1^{1/3} + 1/q_2^{1/3}))$; this form is superior when $\min(q_1, q_2) = \omega(\sqrt{\ln q}\, q^{2/3})$. Any channel such as the binary symmetric, unidirectional, or half-lie channel that is closed under prefixes has this property, for example. We are optimistic that Theorem 3.8 could provide a basis for understanding the case in which the number of lies grows to infinity, or for improving bounds on the best known k-error-correcting and radius k covering codes.

Acknowledgments

The idea for this paper grew from combining a question posed by Nathan Linial in 2005: "Does it matter if Carole is using a Z-channel for her lies but Paul does not know which one?", with our presumption that there should be a liar game corresponding to adaptive block codes with unidirectional errors. After completing this work, we were informed of the extension [15] of [6], which is a specialization of the original liar game case of Theorem 2.3. We thank Ioana Dumitriu, Joel Spencer, Alexander Vardy, and Ilya Dumer for several helpful discussions. We especially thank the anonymous referee for carefully reviewing the original manuscript and detecting several issues.

References

[1] A. Rényi, On a problem in information theory, Magyar Tud. Akad. Mat. Kutató Int. Közl. 6 (1961) 505–516 (1962).
[2] S.M. Ulam, Adventures of a Mathematician, Charles Scribner's Sons, New York, 1976.
[3] A. Pelc, Solution of Ulam's problem on searching with a lie, J. Combin. Theory Ser. A 44 (1) (1987) 129–140.
[4] E.R. Berlekamp, Block coding for the binary symmetric channel with noiseless, delayless feedback, in: Error Correcting Codes, Proc. Sympos. Math. Res. Center, Madison, WI, 1968, John Wiley, New York, 1968, pp. 61–88.
[5] I. Dumitriu, J. Spencer, The two-batch liar game over an arbitrary channel, SIAM J. Discrete Math. 19 (4) (2005) 1056–1064 (electronic).
[6] R. Ahlswede, F. Cicalese, C. Deppe, Searching with lies under error cost constraints, Discrete Appl. Math. 156 (2008) 1444–1460.
[7] R.B. Ellis, C.H. Yan, Ulam's pathological liar game with one half-lie, Int. J. Math. Math. Sci. 2004 (29–32) (2004) 1523–1532.
[8] R.B. Ellis, V. Ponomarenko, C.H. Yan, The Rényi–Ulam pathological liar game with a fixed number of lies, J. Combin. Theory Ser. A 112 (2) (2005) 328–336.
[9] G. Fang, H.C.A. van Tilborg, Bounds and constructions of asymmetric or unidirectional error-correcting codes, Appl. Algebra Engrg. Comm. Comput. 3 (4) (1992) 269–300.
[10] P.R.J. Östergård, E.A. Seuranen, Unidirectional covering codes, IEEE Trans. Inform. Theory 52 (1) (2006) 336–340.
[11] N. Alon, J.H. Spencer, The Probabilistic Method, second ed., John Wiley & Sons, New York, 2000.
[12] V.S. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory, vols. I, II, North-Holland, Amsterdam, 1998.
[13] D.N. Gevorkyan, On nonbinary codes with fixed code distance, in: Proc. 5th Int. Symp. Information Theory, Moscow–Tbilisi, 1979, pp. 93–96 (in Russian).
[14] S. Yekhanin, I. Dumer, Long nonbinary codes exceeding the Gilbert–Varshamov bound for any fixed distance, IEEE Trans. Inform. Theory 50 (10) (2004) 2357–2362.
[15] R. Ahlswede, F. Cicalese, C. Deppe, U. Vaccaro, Two batch search with weighted lie cost, IEEE Trans. Inform. Theory 55 (4) (2009) 1433–1439.