On the multi-interval Ulam-Rényi game: For 3 lies 4 intervals suffice

Ferdinando Cicalese and Massimiliano Rossi

Department of Computer Science, University of Verona, Italy
ferdinando.cicalese@univr.it, massimiliano.rossi_01@univr.it

Abstract. We study the problem of identifying an initially unknown m-bit number by using yes-no questions when up to a fixed number e of the answers can be erroneous. In the variant we consider here questions are restricted to be the union of up to a fixed number of intervals.
For any $e \geq 1$ let k_e be the minimum k such that for all sufficiently large m, there exists a strategy matching the information theoretic lower bound and only using k-interval questions. It is known that $k_e = O(e^2)$. However, it has been conjectured that the $k_e = \Theta(e)$. This *linearity conjecture* is supported by the known results for small values of e. For $e \leq 2$ we have $k_e = e$. We extend these results to the case $e = 3$. We show $k_3 \leq 4$ improving upon the previously known bound $k_3 \leq 10$.

1 Introduction

In the **Ulam-Rényi game with multi-interval questions,** two players, called Questioner and Responder—for reasons which will become immediately clear—fix three integer parameters: $m \geq 0$, $e \geq 0$ and $k \geq 1$. Then, Responder chooses a number x from the set $\mathcal{U} = \{0, 1, \ldots, 2^m - 1\}$, and keeps it secreto to Questioner. The task of Questioner is to identify the *secret* number x chosen by Responder asking k-interval queries. These are *yes-no* membership questions of the type "Does x belong to Q?" where Q is any subset of the search space *which can be expressed as the union of* $\leq k$ *intervals*. We identify a question with the subset Q. Therefore, the set of allowed questions is given by the family of sets:

$$\mathcal{T} = \left\{ \bigcup_{i=1}^{k} \{a_i, a_i + 1, \ldots, b_i\} \mid 0 \leq a_1 \leq b_1 \leq a_2 \leq b_2 \leq \cdots \leq a_k \leq b_k < 2^m \right\}.$$

Responder tries to make Questioner's search as long as possible. To this aim, Responder can adversarially lie up to e times during game i.e., by answering *yes* to a question whose correct answer is *no* or vice versa.

For any m and e let $N_{\min}(2^m, e) = \min\{q \mid 2^{q-m} \geq \sum_{i=0}^{e} \binom{q}{i}\}$. It is known that in a game over a search space of cardinality $n = 2^m$ and e lies allowed to Responder, $N_{\min}(2^m, e)$ is a lower bound on the number of questions that Questioner has to ask in order to be sure to identify Responder's secret number (see, e.g., [3]). This lower bound holds in the version of the game in which

Questioner's questions can refer to any subset, without the restriction to k-interval queries. A fortiori, the lower bound holds for the multi-interval game for any value of k. Strategies of size $N_{\min}(2^m, e)$, i.e., matching the information theoretic lower bound, are called *perfect*.

It is known that for any $e \geq 0$ and up to finitely many exceptional values of m, Questioner can infallibly discover Responder's secret number asking $N_{\min}(2^m, e)$ questions. However, in general such *perfect* strategies rely on the availability of arbitrary subset questions, i.e., any subset of the search space [20].

When the cardinality of the search space is 2^m the description of an arbitrary subset query requires 2^m bits. Moreover, in order to implement the known strategies using $N_{\min}(2^m, e)$ queries, $\Theta(e2^m)$ bits are necessary to record the intermediate *states* of the game (see the next section for the details). In contrast, a k-interval-query can be expressed by simply providing the boundaries of the k-intervals defining the question, hence reducing the space requirements of the strategy to only $2k \cdot m$ bits.

On the basis of these considerations, we will focus on the following problem:

Main question. For given $e \geq 0$, denote by k_e the smallest integer k such that for all sufficiently large m Questioner has a perfect strategy in the multi-interval game over the set of m-bit numbers only using k-interval queries. What is the value of k_e for $e = 1, 2, \ldots$?

In [14] it was proved that for $e = 2$ for any $m \geq 0$ (up to finitely many exceptions) there exists a searching strategy for Questioner of size $N_{\min}(m, e)$ (hence perfect) only using 2-interval questions, and, conversely, perfect strategies which only use 1-interval questions cannot generally exist. The case $e = 1$ is analysed in [6] where it is shown that perfect strategies exists for $e = 1$ even when only using 1-interval questions. However, comparison questions—of the type "Is $x \leq q$?"—are not powerful enough to provide perfect strategies for the case $e = 1$ [19, 2].

These results show that for $e \leq 2$, the answer to our main question is $k_e = e$.

In [6] one of the authors proved that for any $e \geq 1$ there exists $k = O(e^2)$ such that for all sufficiently large m Questioner can identify an m-bit number by using exactly $N(2^m, e)$ k-interval questions when Responder can lie at most e times. In [6] also conjectured that $k_e = O(e)$ interval might suffice for any e and all sufficiently large m. We will refer to this as the *linearity conjecture*.

Our result. We focus on the case $e = 3$. We show that for any sufficiently large m, there exists a strategy to identify an initially unknown m-bit number when up to 3 answers are lies, which matches the information theoretic lower bound and only uses 4-interval queries. With respect to the main question above, we are showing here that $k_3 \leq 4$. This way we significantly improve the best previously known bound of [6] yielding $k_3 \leq 10$. We note that the main tool we employ in the analysis (Lemma 2) naturally lends itself to a generalization to any fixed e. Ongoing research is about a stronger form of Theorem 1 that together with such a generalized version of Lemma 2 might lead to the proof of the linearity conjecture mentioned above, i.e., $k_e = O(e)$. Because of space constraints some proofs are omitted. The complete version can be found at arXiv:1708.08738 [math.CO]

Related work. The Ulam-Rényi game [21, 18] has been extensively studied in various contexts including error correction codes [1, 3, 10, 7], learning [4, 9, 16], many-valued logics [8, 10], wireless networks [13], psychophysics [12], and, principally, sorting and searching in the presence of errors (for the large literature on this topic, and the several variants studied, we refer the reader to the survey papers [8, 17] and the book [5]).

2 Basic facts

From now on we concentrate on the case $e = 3$ and the 4-interval questions. Let Q be the subset defining the question asked by Questioner. Let $\overline{Q}$ be the complement of Q, i.e., $\overline{Q} = \{0, 1, \ldots, 2^m - 1\} \setminus Q$.

If Responder answers *yes* to question Q, then we say that any number $y \in Q$ *satisfies* the answer and any $y \in \overline{Q}$ *falsifies* the answer. If Responder answers *no* to question Q, then we say that any number $y \in \overline{Q}$ *satisfies* the answer and any $y \in Q$ *falsifies* the answer.

For each $y \in U$, we define $\sigma(y)$ as the number of answers falsified by y, truncated at 4. For each $i = 0, 1, \ldots, 3$, we will also write $\sigma^{-1}(i)$ to denote the set of numbers falsifying exactly i of Responder's answers. And define $\sigma^{-1}(4) = \sigma^{-1}(> 3)$ to denote the set of numbers that as a result of the answers received cannot be Responder's secret number.

States and supports. A *state* is a map $\sigma : \mathcal{U} \to \{0, 1, 2, 3, 4\}$. The *type* of σ is the quadruple $\tau(\sigma) = (t_0, t_1, t_2, t_3)$ where $t_i = |\sigma^{-1}(i)|$ for each $i = 0, 1, 2, 3$. The *support* Σ of σ is the set of all $y \in \mathcal{U}$ such that $\sigma(y) < 4$. A state is *final* iff its support has cardinality at most one. The *initial state* α is the function mapping each element of $\mathcal{U}$ to 0. We formalise the dynamics of states as follows:

Answers and resulting states. Let σ be the current state with support Σ and Q be the new question asked by Questioner. Let $b \in \{yes, no\}$ be the answer of Responder. Define the answer function $b : \Sigma \to \{0, 1\}$ associated to question Q by stipulating that $b(y) = 0$ if and only if y satisfies answer b to question Q. Then, the resulting state σ_b is given by $\sigma_b(y) = \max\{\sigma(y) + b(y), 4\}$.

More generally, starting from state σ after questions $Q_1, \ldots, Q_t$ with answers $b_1, \ldots, b_t$ the resulting state is $\sigma_{b_1\, b_2 \cdots b_t} = \max\{\sigma(y) + \sum_{j=1}^{t} b_j(y), 4\}$.

In particular, for σ being the initial state we have that the resulting state after t questions is the truncated sum of the corresponding answer functions associated to Responder's answers.

Strategies. A strategy of size q is a complete binary tree of depth q where each internal node ν maps to a question Q_ν. The left and right branch stemming out of ν map to the function answers *yes* and *no* associated to question Q_ν. Each leaf ℓ is associated to the state σ^ℓ resulting from the sequence of questions and answers associated to the nodes and branches on unique path from the roof to ℓ. In particular, if $b_1, \ldots, b_q$ are the answers/branches leading to ℓ then we have $\sigma^\ell = \alpha_{b_1 \cdots b_q}$ as defined above.

The strategy is *winning* iff for all leaves ℓ we have that σ^ℓ is a final state.

We can also extend the above definition to an arbitrary starting state. Given a state σ, we say that a strategy $\mathcal{S}$ of size q is winning for σ if for any root to leaf path in $\mathcal{S}$ with associated answers $b_1, \ldots, b_q$ the state $\sigma_{b_1 \cdots b_q}$ is final .

We define the *character* of a state σ as $ch(\sigma) = \min\{q \mid w_q(\sigma) \leq 2^q\}$, where $w_q(\sigma) = \sum_{j=0}^{3} |\sigma^{-1}(j)| \sum_{\ell=0}^{3-j} \binom{q}{\ell}$ is referred to as the *qth volume* of σ.

We have that the lower bound $N_{\min}(2^m, e)$, mentioned in the introduction, coincides with the character of the initial state α, such that $\alpha^{-1}(0) = \mathcal{U}$ and $\alpha^{-1}(i) = \emptyset$ for $i = 1, 2, 3, 4$ (see Proposition 1 below). Notice also that a state has character 0 if and only if it is a final state.

For a state σ and a question Q let σ_{yes} and σ_{no} be the resulting states according to whether Responder answers, respectively, yes or no, to question Q in state σ. Then, from the definition of the qth volume of a state, it follows that for each $q \geq 1$, we have $w_q(\sigma) = w_{q-1}(\sigma_{yes}) + w_{q-1}(\sigma_{no})$. A simple induction argument gives the following lower bound [3].

Proposition 1. *Let σ be the state of the game. For any integers $0 \leq q < ch(\sigma)$ and $k \geq 1$, starting from state σ, Questioner cannot determine Responder's secret number asking only q many k-interval-queries.*

In order to finish the search within $N_{\min}(2^m, e)$ queries, Questioner has to guarantee that each question asked induces a strict decrease of the character of the state of the game. The following lemma provides a sufficient condition for obtaining such a strict decrease of the character.

Lemma 1. *Let σ be the current state, with $q = ch(\sigma)$. Let D be Questioner's question and σ_{yes} and σ_{no} be the resulting states according to whether Responder answers, respectively, yes or no, to question D.*

If $|w_{q-1}(\sigma_{yes}) - w_{q-1}(\sigma_{no})| \leq 1$ then $ch(\sigma_{yes}) \leq q - 1$ and $ch(\sigma_{no}) \leq q - 1$.

A question which satisfies the hypothesis of Lemma 1 will be called *balanced*. A special case of balanced question is obtained when for a state σ the question D satisfies $|D \cap \sigma^{-1}(i)| = |\sigma^{-1}(i)|/2$ for each $i = 0, \ldots, e$. In this case, we also call the question an *even splitting*.

Intervals and 4-interval-question. An interval in $\mathcal{U}$ is either the empty set $\emptyset$ or a set of consecutive elements $[a, b] = \{x \in \mathcal{U} | a \leq x \leq b\}$. The elements a, b are called the boundaries of the interval.

A 4-interval question (or simply a question) is any subset Q of $\mathcal{U}$ such that $Q = I_1 \cup I_2 \cup I_3 \cup I_4$ where for $j = 1, 2, 3, 4$, I_j is an interval in $\mathcal{U}$.

The *type of* Q, denoted by $|Q|$, is the quadruple $|Q| = [a_0^Q, a_1^Q, a_2^Q, a_3^Q]$ where for each $i = 0, 1, 2, 3$, $a_i^Q = |Q \cap \sigma^{-1}(i)|$.

Following [14] we visualize the search space as a necklace and restrict it to the set of number which are candidate to be the secret number, i.e., we identify $\mathcal{U}$ with its support $\Sigma = \mathcal{U} \cap \bigcup_{i=0}^{3} \sigma^{-1}(i)$.

For any non-final state, i.e., $|\bigcup_{i=0}^{3} \sigma^{-1}(i)| > 1$, for each $x \in \bigcup_{i=0}^{3} \sigma^{-1}(i)$ we define the successor of x to be the number $x + r \mod 2^m$ for the smallest $0 < r < 2^m$ such that $x + r \mod 2^m \in \bigcup_{i=0}^{3} \sigma^{-1}(i)$. In particular, for the initial state 0 is the successor of $2^m - 1$.

For $a, b \in \bigcup_{i=0}^{3} \sigma^{-1}(i)$ we say that there is an arc from a to b and denote it by $\langle a, b\rangle$ if the following two conditions hold: (i) $\sigma(x) = \sigma(a)$ for each element x encountered when moving from a to b in $\mathcal{U}$ passing from one element to its successor; (ii) $\sigma(c) \neq \sigma(a)$ and $\sigma(d) \neq \sigma(b)$ where a is the successor of c and d is the successor of b. We say that arc $\langle a, b\rangle$ is on level $\sigma(a)$ and call a and b the left and right boundary of the arc.

In words, an arc is a maximal sequence of consecutive elements lying on the same level of the state σ.

For the sake of definiteness, we allow an arc to be empty. Therefore, we can associate to a state σ a smallest sequence $\mathcal{L}^\sigma$ of (possibly empty) arcs $a_0, \ldots, a_{r-1}$ such that for each i the levels of arcs a_i and a_{i+1} differ exactly by 1. Note that, by requiring that the length r be minimum the sequence $\mathcal{L}^\sigma$ is uniquely determined up to circular permutation.

For each $i = 0, 1, \ldots, r$, we say that arcs a_i and $a_{(i+1) \bmod r}$ are *adjacent* (or *neighbours*). We say that a_i is a *saddle* if both adjacent arcs are on a lower level, i.e., $a_{(i-1) \bmod r}, a_{(i+1) \bmod r} \in \sigma^{-1}(k-1)$ and $a_i \in \sigma^{-1}(k)$ for some k

We say that a_i is a *mode* if both adjacent arcs are on a higher level, i.e., $a_{(i-1) \bmod r}, a_{(i+1) \bmod r} \in \sigma^{-1}(k+1)$ and $a_i \in \sigma^{-1}(k)$ for some k

We say that a_i is a *step* if for some k $a_i \in \sigma^{-1}(k)$ and either $a_{(i-1) \bmod r} \in \sigma^{-1}(k-1), a_{(i+1) \bmod r} \in \sigma^{-1}(k+1)$ or $a_{(i-1) \bmod r} \in \sigma^{-1}(k+1), a_{(i+1) \bmod r} \in \sigma^{-1}(k-1)$.

Based on the above notions, we now define a well-shaped state for e lies.

Definition 1. *Let σ be a state and $\mathcal{L}^\sigma$ be its associated list of arcs. Then, σ is* ***well shaped*** *iff the following conditions hold:*

- *for $i = 0, \ldots, e-1$, in $\mathcal{L}^\sigma$ there are exactly $(2i+1)$ arcs lying on level i.*
- *in $\mathcal{L}^\sigma$ there are exactly e arcs lying on level e.*

It is not hard to see that for the case $e = 3$ under investigation, the only two feasible well-shaped states are described as follow: $\sigma^{-1}(0)$ is an arc S in Σ; $\sigma^{-1}(1)$ is the disjoint union of three arcs H,N and O in Σ with N and O adjacent to S; $\sigma^{-1}(2)$ is the disjoint union of five arcs A, B, C, L and M in Σ with B and C adjacent to H, L adjacent to N; $\sigma^{-1}(3)$ is the disjoint union of three arcs P, Q, R in Σ with R and P adjacent to A.

Starting with S and scanning $\mathcal{U}$ with positive orientation, we can list the twelve arcs (restricted to Σ) in one of the following two possibilities:

$$\sigma_1 = L^2 N^1 S^0 O^1 M^2 Q^3 B^2 H^1 C^2 R^3 A^2 P^3 \tag{1}$$

$$\sigma_2 = L^2 N^1 S^0 O^1 B^2 H^1 C^2 Q^3 M^2 R^3 A^2 P^3 \tag{2}$$

where for an arc X the notation X^i denotes that $X \subseteq \sigma^{-1}(i)$.

Typical well-shaped states of type (1) and (2) are shown in Figures 1 and 2 respectively.

Let σ be a state and $\langle a, b\rangle$ be a non-empty arc of σ.

We say that a question Q splits the arc $\langle a, b\rangle$ if there exists an interval I in Q that intersects $\langle a, b\rangle$ and contains exactly one of its boundaries a, b. In words,

there is an interval in the question such that some non-empty part of the arc satisfies a yes answer and some non-empty part of the arc satisfies a no answer.

If a question Q splits exactly one arc on level i of σ according to whether such an arc is a mode, a saddle, or a step, we say that *at level i* the question Q (or, equivalently, an interval of Q) is *mode-splitting*, *saddle-splitting*, *step-splitting*, respectively.

Let Q be a *step-splitting* question at level i. Let $\langle a, b\rangle$ be the arc at level i which is split by an interval I of Q. Then, by definition I contains exactly one of the boundaries of the arc. If I contains the boundary of the arc that flanks an arc at level $i+1$ we say that Q (or, equivalently, an interval of Q) is *downward step-splitting*; if I contains the boundary of the arc that flanks an arc at level $i-1$ we say that Q (or, equivalently, an interval of Q) is *upward step-splitting*.

We say that a question Q *covers entirely* the arc $\langle a, b\rangle$ if $[a, b]$ is contained in one of the intervals defining Q.

If a question Q covers entirely an arc on level i of σ according to whether such an arc is a mode, a saddle, a step, we say that *at level i* the the question Q (or, equivalently, an interval of Q) is *mode-covering*, *saddle-covering*, *step covering*, respectively.

Refer to Figure 3 for a pictorial representation of the interval types and questions effect on states.

We will be interested in having questions that guarantee that both the two possible states resulting from the answer yes and no are well-shaped. We will define conditions on the intersection between the intervals defining the question and the arcs of a (well-shaped) state σ such that the both σ^{yes} and σ^{no} are well shaped. It turns out that this condition can be defined locally, level by level and arc by arc.

Lemma 2. *Given a well-shaped state σ and a question Q, if the following conditions are satisfied then both σ_{yes} and σ_{no} are well-shaped. For each $i = 0, 1, 2$*

(a) At most one arc is splitted on level i
(b) Exactly one of the following holds
  (i) at level i the question Q is mode-splitting;
  (ii) at level i the question Q is upward step-splitting and mode-covering.
  (iii) at level i the question Q is downward step-splitting and a mode is completely uncovered—equivalently the complementary question $\overline{Q}$ is mode-covering at level i.
  (iv) at level i the question Q is saddle-splitting and mode-covering and there is also a mode completely uncovered—equivalently the complementary question $\overline{Q}$ is mode-covering at level i.
(c) If besides the condition in (b) the question Q is also saddle-covering then Q also covers a mode different from the one possibly used to satisfy (b).

3 A key result on the existence of 4-interval questions

The strategy we propose is based on the approach of Spencer [20]. We are going to recall the strategy presented in [20] and prove how to implement questions

in that strategy by means of 4-interval questions. The main technical tool will be to show that we can define 4-interval balanced questions and also guarantee that each intermediate state is well-shaped.

In this section, we will characterise questions in terms of the ratio between the components of the question and the components of the state they are applied. We will show conditions for the existence of questions that can be implemented using only 4-intervals and such that the resulting states are *well-shaped* whenever the state they are applied to is well shaped.

For each of them, we show how to select the exact amount of elements in the query among the arcs representing the state. Then, we prove that no other cases are allowed and finally we show that the well shapeness property of the state is preserved in both states resulting from the answer to the query.

Theorem 1. *Let σ be a well-shaped state of type $\tau(\sigma) = (a_0, b_0, c_0, d_0)$. Let a, b, c, d be integers such that:*

$$0 \leq a \leq a_0 \quad 0 \leq b \leq \lceil \frac{1}{2} b_0 \rceil \quad 0 \leq c \leq \lceil \frac{1}{2} c_0 \rceil \quad 0 \leq d \leq \lceil \frac{2}{3} d_0 \rceil$$

Then there exists a 4-interval question Q of type $|Q| = [a, b, c, d]$ that we can ask in state σ and such that both the resulting "yes" and "no" states are well-shaped*.*

Proof. We first show how to select the intervals of the question Q in order to satisfy the desired type. We proceed level by level. For each $i = 0, 1, 2, 3$, we show how to select up to 4 intervals that cover the required number of elements in the first i levels. For each level $i = 0, 1, 2, 3$ we record in a set $\mathcal{E}(i)$ the extremes of the intervals selected so far that have a neighbour on the next level. We refer to the elements in $\mathcal{E}(i)$ as the boundaries at level i. When processing the next level, we try to select arc neighbouring the elements in $\mathcal{E}(i)$ since this means we can cover elements at the new level without using additional intervals. Arguing with respect to such boundaries, we show that the (sub)intervals selected at all level can be merged into at most 4 intervals. Hence the resulting question Q is a 4-interval question. Finally, we will show that asking Q in σ both the resulting states are well-shaped states.

Recall the arc notation used in (1)-(2). In our construction, a special role will be played by the arcs S, H, A, which are the greatest mode respectively of level $0, 1$ and 2, and the larger between their two neighbouring arcs at the level immediately below. Therefore, let us denote by $A^{(1)}$ the larger arc between N and O; we denote by $A^{(2)}$ be the larger arc between B and C; and finally, we denote by $A^{(3)}$ the larger arc between R and P.

Moreover, we denote by s^+ the boundary between S and $A^{(1)}$ and with s^- the other boundary of S.

Analogously, we denote by h^+ the boundary between H and $A^{(2)}$ and with h^- the other boundary of H.

We denote by a^+ the boundary between A and $A^{(3)}$ and with a^- the other boundary of A.

Level 0 For any $0 < a \leq a_0$ there exists $s^* \in S$ such that denoting by S^* the sub-arc of S between s^* and s^+ we have that $|S^*| = a$ and the boundary of S^* includes s^+. Then we have $\mathcal{E}(0) \supseteq \{s^+\}$.
Therefore, with one interval $I^{(0)} = S^*$ we can accommodate the a elements on level 0 and guarantee that this interval has an extreme at s^+.
Moreover, the interval $I^{(0)}$ on arc S is a mode-splitting interval.

Level 1 By the assumption $b \leq \lceil \frac{1}{2} b_0 \rceil$, and the definition of $A^{(1)}$ it follows that $b \leq |A^{(1)}| + |H|$. We now argue by cases

(a) $b \leq |H|$. Then there exists h^* in H such that the sub-arc $H^* \subseteq H$ between h^* and h^+ satisfies $|H^*| = b$ and we can cover it with one interval $I^{(1)}$ with a boundary at h^+.

(b) $|H| < b \leq |H| + |A^{(1)}|$. Then, there exists $x_1^* \in A^{(1)}$ such that letting $X^{(1)}$ be the sub-arc of $A^{(1)}$ between x_1^* and s^+, we have $|X^{(1)}| + |H| = b$ and we can cover these b elements extending the previously defined $I^{(0)}$ so that it covers $X^{(1)}$ too and having $I^{(1)} = H$. In this case we have that the boundaries of $I^{(1)}$ are both h^+ and h^-.

Summarising, we can cover the a elements on level 0 and the b elements on level 1 with at most two intervals and guarantee that the boundaries of these intervals include h^+.
Moreover either the interval $I^{(1)}$ on arc H is a mode-splitting interval or the interval $I^{(1)}$ covers entirely the mode H and the interval $I^{(0)}$ on arc $A^{(1)}$ is a step-splitting interval.
Therefore the choice of the intervals so far satisfies conditions in Lemma 2.

Level 2 Again we argue by cases

(a) $c \leq |A|$. Then, there exists a^* in A such that letting A^* be the sub-arc of A between a^* and a^+ we have $|A^*| = c$ and we can cover it with one interval $I^{(2)} = A^*$ with one boundary in a^+.

(b) $|A| < c \leq |A| + |A^{(2)}|$ Then, there exists $x^* \in A^{(2)}$ such that letting $X^{(2)}$ be the sub-arc of $A^{(2)}$ between x^* and h^+, we have $|X^{(2)}| + |A| = c$ and we can cover these c elements extending the previously defined $I^{(1)}$ so that it covers $X^{(2)}$ too and having $I^{(2)} = A$. In this case we have that the boundaries of $I^{(2)}$ are both a^+ and a^-.

(c) $c > |A| + |A^{(2)}|$. Let E denote the largest arc on level 2 not in $\{A^{(2)}, A\}$. Then, by the definition of $A^{(2)}$ we have that $|A| + |A^{(2)}| + |E| \geq |Y| + |Z|$ where Y and Z denote the arcs on level 2 not in $\{A, A^{(2)}, E\}$. This is true because, at least one of the arcs Y, Z is not larger than $A^{(2)}$ and the other one is not larger than E.
Then, by the assumption $c \leq \lceil \frac{c_0}{2} \rceil$ it follows that $|A| + |A^{(2)}| + |E| \geq c$.
Let z be the boundary of $A^{(2)}$ on the opposite side with respect to H.
Let e^+ be the boundary between E and a neighbouring arc at level 3 or at level 1 according to whether z is flanking an arc at level 1 or an arc at level 3—with reference to Figures 1, 2, is an easy direct inspection shows that such a choice is always possible.
Therefore, there exists $e^* \in E$ such that letting E^* be the sub-arc of E between e^* and e^+ we have $|A| + |A^{(2)}| + |E^*| = c$ and we can cover the corresponding set of elements by: (i) extending $I^{(1)}$ from h^+ and have it

include the whole $A^{(2)}$; (ii) defining $I^{(2)} = A$; defining a fourth interval $I^{(3)} = E^*$. Therefore, we have that the boundaries of $I^{(2)}$ are both a^+ and a^- and, in the case of a σ of type in Fig. 2, the boundary of $I^{(3)}$ includes e^+, and the boundary of $I^{(1)}$ is the boundary z of the arc $A^{(2)}$ where this joins its adjacent arc at level 3.

Summarising, we can cover the a elements on level 0 and the b elements on level 1 and the c elements of level 2 with at most four intervals. More precisely, if, proceeding as above we only use three intervals, $I^{(0)}, I^{(1)}, I^{(2)}$, (and set $I^{(3)} = \emptyset$), we also guarantee that the boundaries of these intervals include a^+. On the other hand, if we use four intervals, (in particular, $I^{(3)} \neq \emptyset$) we have that the boundaries of these intervals include a^+, a^- and exactly one between e^+, z. Therefore $\{a^+, a^-\} \subset \mathcal{E}(2) \subset \{a^+, a^-, z, e^+\}$. Notice that, since there are only three arcs at level 3; in the case where $I^{(3)} \neq \emptyset$ either there is an arc on level 3 with both ends neighbouring the boundaries in $\mathcal{E}(2)$, or each arc on level 3 has one end neighbouring a boundary in $\mathcal{E}(2)$.

Moreover exactly one of the following cases holds (i) the interval $I^{(2)}$ on arc A is a mode-splitting interval; (ii) the interval $I^{(2)}$ covers entirely the mode H and the interval $I^{(1)}$ on arc $A^{(2)}$ is a step-splitting interval; (iii) the interval $I^{(2)}$ covers the mode H, no interval intersects mode M and the interval $I^{(1)}$ on arc $A^{(2)}$ is saddle-splitting; (iv) the interval $I^{(2)}$ covers the mode H and the interval $I^{(1)}$ covers the arc $A^{(2)}$ and the interval $I^{(3)}$ on arc E is downward step-splitting; (v) the interval $I^{(2)}$ covers the mode H, the interval $I^{(1)}$ covers the arc $A^{(2)}$, hence it is saddle-covering, and the interval $I^{(3)}$ on arc E is upward step-splitting. .

In all the above five cases, the (partial) question built so far, with the intervals defined for levels 0, 1, 2, satisfy the conditions of Lemma 2.

Level 3 Let us denote by W, U the two arcs at level 3 which are different from $A^{(3)}$, with $|W| \geq |U|$. Then, by definition we also have $|A^{(3)}| \geq |U|$, hence $|A^{(3)}| + |W| \geq \frac{2}{3} d_0 \geq d$. We now argue by cases:

(a) $d < |A^{(3)}|$. Then, there exists x_3^* in $A^{(3)}$ such that the sub-arc $X^{(3)}$ between a^+ and x_3^* has cardinality $|X^{(3)}| = d$ and can be covered by extending $I^{(2)}$ (which have a boundary at a^+).

(b) $|A^{(3)}| < d \leq |A^{(3)}| + |W|$.
We have two sub-cases:
- $I^{(3)} = \emptyset$. I.e., for accommodating the question's type on Levels 0,1,2, we have only used three intervals. By assumption, there exists a sub-arc W^* of W such that $|W^*| + |A^{(3)}| = d$. Then, defining $I^{(3)} = W^*$, and extending $I^{(2)}$ (as in the previous case) so that it includes the whole of $A^{(3)}$ guarantees that the four intervals $I^{(0)}, \ldots I^{(3)}$ define a question of the desired type.
- $I^{(3)} \neq \emptyset$. Then, by the observations above, as a result of the construction on level 2, either there is an arc on level 3 with both ends at a boundary in $\mathcal{E}(2)$ or each arc on level 3 has a boundary in $\mathcal{E}(2)$. In the latter case, we can clearly extend the intervals $I^{(2)}$ and $I^{(3)}$ in order to cover d elements on level 3. In the former case, let Z denote the arc with both ends at boundaries in $\mathcal{E}(2)$. If $|Z| \geq d$, we can

simply extend $I^{(2)}$ and $I^{(3)}$ towards the internal part of Z until they include d elements of Z. If $|Z| < d$ then we can extend $I^{(2)}$ so that it includes Z and $I^{(3)}$.

Since the way intervals are extended on level 3 do not affect the arc covering and splitting on the previous level, we have that in all cases the resulting 4-interval question satisfies the conditions of Lemma 2, which guarantees that both resulting states are well-shaped. The proof is complete. □

Refer to Figures 1 and 2 for a pictorial representation of the 4-intervals question construction in the proof of Theorem 1.

4 The structure of perfect 4-interval strategies for 3 lies

We now show how to employ the result of the previous section to obtain a perfect strategy for the Ulam-Rényi game with 3 lies, only using 4-interval questions. We show that, for $e = 3$, by only relying on 4-interval questions, we can implement the strategy of [20], that can be summarised as follows:

1. As long as the state satisfies $\sum_{i=0}^{2} |\sigma^{-1}(i)| > 1$ ask a question Q of type $[a_0^Q, a_1^Q, a_2^Q, a_3^Q]$ where, for $i = 0, 1, 2$, $a_i^Q \in \left\{ \lfloor \frac{|\sigma^{-1}(i)|}{2} \rfloor, \lceil \frac{|\sigma^{-1}(i)|}{2} \rceil \right\}$ with the choice of whether to choose floor or ceiling alternating among those levels where $|\sigma^{-1}(i)|$ is odd. The value of a_3^Q is computed based on the choices of a_0^Q, a_1^Q, a_2^Q, in order to guarantee that the resulting question is balanced, i.e., $a_3^Q = \lfloor \frac{1}{2} \sum_{j=0}^{2} (|\sigma^{-1}(j)| - 2a_j^Q) \binom{q}{j} \rfloor$, where $q + 1$ is the character of σ;
2. when the state satisfies $\sum_{i=0}^{2} |\sigma^{-1}(i)| \leq 1$, ask a balanced question Q of type $[0, 0, 0, a_3^Q]$.

The condition in 2. can be easily guaranteed. In fact, the following proposition shows that questions in point 2. are implementable by 4-interval questions, preserving the well-shape of the state.

Proposition 2. *Let σ be a well-shaped state with $\sigma^{-1}(3) > 0$ and $\sum_{i=0}^{2} |\sigma^{-1}(i)| \leq 1$. Let $ch(\sigma) = q$. Then, starting in state σ the Questioner can discover the Respounder's secret number asking exactly q many 1-interval-queries.*

The main point in the argument of [20] is that, up to finitely many exceptions, for all $m = \log |\mathcal{U}|$, the value a_3^Q defined in 1. is feasible, in the sense that using the above rules yields $0 \leq a_3^Q \leq |\sigma^{(-1)}(3)|$.

We can now employ Theorem 1 to show that the above strategy can be implemented by a 4-intervals-question. Let Q be the question defined in 1. Let $\overline{Q}$ be the complementary question, and $[a_0^{\overline{Q}}, a_1^{\overline{Q}}, a_2^{\overline{Q}}, a_3^{\overline{Q}}]$ denote its type. For $i = 0, 1, 2$, we have $a_i^Q, a_i^{\overline{Q}} \leq \lceil \frac{|\sigma^{-1}(i)|}{2} \rceil$. Moreover, we have $\min\{a_3^Q, a_3^{\overline{Q}}\} \leq \lceil \frac{2}{3} |\sigma^{-1}(3)| \rceil$. Therefore, asking Q or $\overline{Q}$ according to whether $a_3^Q \leq a_3^{\overline{Q}}$ guarantees that the question satisfies the hypothesis of Theorem 1 and then it can be implemented as 4-interval question which also preserves the well-shape of the state.

We can summarise our discussion in the following theorem.

Theorem 2. *For all sufficiently large m in the game played over the search space $\{0, \ldots, 2^m - 1\}$ with 3 lies, there exists a* perfect *4-intervals strategy. In particular, the strategy uses at most $N_{\min}(2^m, 3)$ questions and all the states of the game are well shaped, hence representable by exactly $12 \log m$ bits (12 numbers from $\mathcal{U}$).*

References

1. R. Ahlswede, F. Cicalese, C. Deppe, and U. Vaccaro, Two Batch Search with Lie Cost. *IEEE Transaction on Information Theory*, **55** (4), pp. 1433–1439, 2009.
2. V. Auletta, A. Negro, G. Parlati. Some results on searching with lies. In: *Proc. of 4th Italian Conf. on Theoretical Computer Science*, pp. 241737, 1992.
3. E.R. Berlekamp. Block coding for the binary symmetric channel with noiseless, delayless feedback. In *Error-Correcting Codes*, Wiley, New York, 61–68, 1968.
4. N. Cesa-Bianchi, Y. Freund, D.P. Helmbold, D. Haussler, R. Schapire, M.K. Warmuth. How to use expert advice. *Journal of the ACM*, **44** (3), pp. 427-485, 1997.
5. F. Cicalese, Fault-Tolerant Search Algorithms, Springer-Verlag, 2013.
6. F. Cicalese. Perfect Strategies for the Ulam-Rényi Game with Multi-interval Questions. *Theory of Computing Systems*, **54** (4), pp. 578-594, 2014.
7. F. Cicalese, U. Vaccaro. Optimal strategies against a liar. TCS 230, 167-193, 2000.
8. F. Cicalese, D. Mundici, and U. Vaccaro, Rota-Metropolis cubic logic and Ulam-Rényi games. In: *Algebraic Combinatorics and Computer Science—A Tribute to Giancarlo Rota*, H. Crapo, D. Senato (Eds.). Springer Italia, pp. 197-244, 2001.
9. F. Cicalese and D. Mundici. Learning and the Art of Fault-tolerant Guesswork. In: *Adaptivity and Learning*, Springer, 115-140, 2003.
10. F. Cicalese, D. Mundici. Recent Developments of Feedback Coding and Its Relations with Many-Valued Logic. In *Proof, Computation and Agency*, J. van Benthem *et al.* (eds.). Springer–Verlag Synthese Library, **352** (3) pp. 115–131, 2011.
11. W. Guzicki, "Ulam's searching game with two lies," *JCT-A*, 54, 1–19, 1990.
12. E. Kelareva, J. Mewing, A. Wirth. Adaptive psychophysical procedures, loss functions, and entropy. *Attention, Perception, and Psychophysics*, 72, 2003–12, 2010.
13. W. Kozma and L. Lazos. Dealing with liars: Misbehavior identification via Rényi-Ulam games. In *Proc. of the 5th Int. ICST Conf. on Security and Privacy in Communication Networks (SecureComm 2009)*, LNICST **19**, pp. 207-17227, 2009.
14. D. Mundici, A. Trombetta. Optimal comparison strategies in Ulam's searching game with two errors. *Theoretical Computer Science*, **182** pp. 217-232, 1997.
15. A. Negro and M. Sereno, "Ulam's searching game with three lies," *Advances in Applied Mathematics*, vol. 13, no. 4, pp. 404–428, 1992.
16. M.B. Or and A. Hassidim. The Bayesian Learner is Optimal for Noisy Binary Search (and Pretty Good for Quantum as Well). In *FOCS'08*, 221–230, 2008.
17. A. Pelc. Searching games with errors—Fifty years of coping with liars. *Theoretical Computer Science*, **270** (1-2) pp. 71-109, 2002.
18. A. Rényi. On a problem of information theory. *MTA Mat. Kut. Int. Kozl. 6B*, pp. 505–516, 1961.
19. J. Spencer. Guess a number with Lying. *Math. Magazine*, **57** pp. 105–108, 1984.
20. J. Spencer. Ulam's searching game with a fixed number of lies. *Theoretical Computer Science*, **95** pp. 307–321, 1992.
21. S.M. Ulam. *Adventures of a Mathematician*, Scribner's, New York, 1976.

A Figures

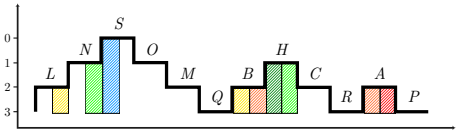

Fig. 1: A well-shaped state of type (1)

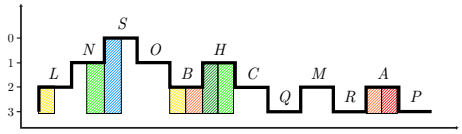

Fig. 2: A well-shaped state of type (2)

The figures provide a pictorial representation of (a) the well-shaped states of type (1) and (2), and of (b) the 4-intervals question construction in the proof of Theorem 1. In Figure 1, arcs S, H, A are *modes* at level $0, 1, 2$, respectively. Arcs Q, R, P are *saddles* at level 3. The remaining arcs are *steps*. On the other hand, in Figure 2, arc B is a saddle at level 2 and arc M is a mode at level 2. We assume the following relative order on the arcs' sizes. On level 1 we assume $N \geq O$ and on level 2 we assume $B \geq C$, $L \geq M$ and $A \geq M$. The questions are depicted for both the feasible well-shaped states for a 3 lies game. Then on level 0 the arc S is split (the light blue question), on level 1 either H is split (the dark green question) or N is split (the dark green and the light green question) and H is covered entirely. On level 2 one of the following holds, either A is split (the red question) or B is split (the orange and red question) and the mode A is covered entirely, or L is split (the yellow, orange and red question) and the mode A is covered entirely. In order to guarantee the well-shapeness preservation, note that in the questions depicted in figure 2 on level 2 the mode M is entirely uncovered, moreover the interval splitting arc L is upward step-splitting in the case of Figure 1 and downward step-splitting in Figure 2.

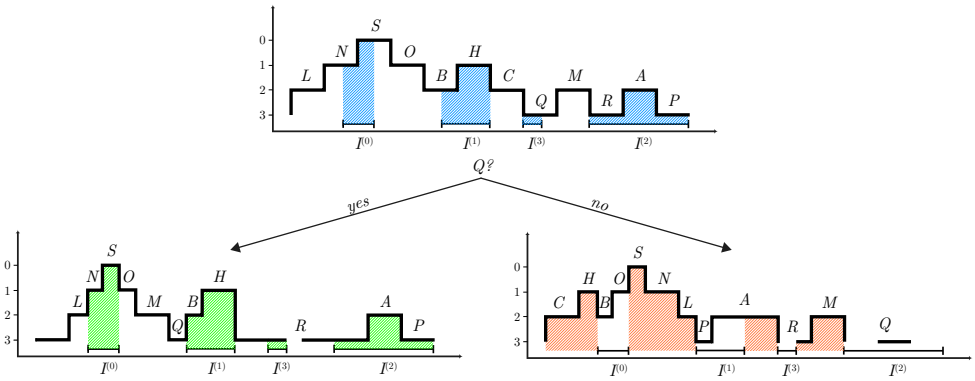

Fig. 3: The figure depicts an example of state dynamics. The question Q is represented by the intervals $I^{(0)}, I^{(1)}, I^{(2)}$ and $I^{(3)}$. The interval I^0 is *mode-splitting* at level 0 and *downward step-splitting* at level 1; $I^{(1)}$ is *mode-covering* at level 1 and *saddle-splitting* at level 2; $I^{(2)}$ is *mode-covering* at level 2 and *saddle-covering* at level 3; $I^{(3)}$ is *saddle-splitting* at level 3. In the resulting states the filled volumes indicate the arcs of the state remained unchanged. The $\sigma^{yes}, \sigma^{no}$ states are represented on the support of the original state σ to show how the elements belonging the lowest level disappear (the blank gaps on the shapes) from the support when they are in contradiction with more than 3 answers.