Searching with lies under error cost constraints

Rudolf Ahlswede [a] Ferdinando Cicalese[b,c, 1] Christian Deppe [a]

[a] *Department of Mathematics, University of Bielefeld, Postfach 100131, D-33501 Bielefeld, Germany*

[b] *Department of Computer Science and Applications, University of Salerno, I-84081 Baronissi (SA), Italy*

[c] *AG Genominformatik, Technische Fakultät, Universität Bielefeld, Germany*

Abstract

The Rényi-Berlekamp-Ulam game is a classical model for the problem of determining the minimum number of queries to find an unknown member in a finite set when up to a finite number of the answers may be erroneous. In the variant considered in this paper, questions with q many possible answers are allowed, further lies are constrained by a bipartite graph with edges weighted by $0, 1, 2, \ldots$ (the "channel"). The channel Γ is an arbitrary assignment stipulating the cost of the different possible lies, i.e., of each answer $j \neq i$ when the correct answer is i by $\Gamma(i, j)$. It is also assumed that a maximum cost e (sum of the cost of all wrong answers) can be afforded by the responder during the whole game. We provide tight asymptotic bounds for the number of questions needed to solve this problem. The appropriate searching strategies are actually provided. We also show that adaptiveness can be dramatically reduced when the channel satisfies certain symmetry constraints.

1 Introduction

The q-ary Rényi-Berlekamp-Ulam game is played by two players, called Paul and Carole. A search space $\mathcal{U} = \{0, \ldots, M-1\}$ is given. Carole chooses a number $x_* \in \mathcal{U}$, the secret number, and Paul must find out x_* by asking the minimum number of q-ary questions. By a q-ary *question* we understand a list $T_0, \ldots, T_{q-1}$ of pairwise disjoint subsets forming a partition of the set $\mathcal{U}$. When presented with such a list, Carole will answer by pointing out a set T_k, supposedly containing the secret number x_*. It is however agreed that Carole may give wrong answers with a total weight up to e. The integer $e \geq 0$ is fixed and known to both players. Intuitively, any q-ary question asks *"Which set among $T_0, T_1, \ldots, T_{q-1}$ does the secret number x_* belong to?"*

[1] Supported by the 2004 Sofja Kovalevskaja Award of the Alexander von Humboldt Stiftung and Bundesministerium für Bildung und Forschung and COMBSTRU a Research Training Network funded through the European Commission

and the answer is just an index $k \in \mathcal{Q} = \{0, 1, \ldots, q-1\}$, meaning that x_* belongs to T_k. We generalize the q-ary game by fixing a function $\Gamma : \mathcal{Q} \times \mathcal{Q} \to \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ such that $\Gamma(i, i) = 0$ for each i, and $\Gamma(i, j) > 0$ for each $i \neq j$. The function Γ is meant to weigh Carole's answers. More precisely, whenever Carole answers j to a question whose correct answer is i, we say that Carole's answer has *individual weight* $\Gamma(i, j)$. Note that every correct answer has weight 0. The parameter e is meant to bound Carole's lies via the following rule:

Carole is allowed to give wrong answers, *with total weight (up to) e.*

Thus, if k is the correct answer to Paul's first question $\mathbf{T} = \{T_0, T_1, \ldots, T_{q-1}\}$, (in the sense that $x_* \in T_k$) then Carole can choose her answer in the set $\{j : e - \Gamma(k, j) \geq 0\}$. If Carole answers i, with i in this set, then her available weight becomes $e - \Gamma(k, i)$. And the *individual weight* of her answer is $\Gamma(k, i)$.

We think of Γ as the weighted noise-transmission pattern on a channel carrying Carole's answers. The q-ary Rényi-Berlekamp-Ulam game with this sort of restriction on the patterns of Carole's lies will be called the *game over the channel* Γ. Each pair (i, j) with $\Gamma(i, j) > e$ stands for an impossible lie: indeed, if Carole answered j to a question whose correct answer is i, already the individual weight of this answer would exceed the total weight e.

The classical q-ary Rényi-Berlekamp-Ulam game is a *Rényi-Berlekamp-Ulam game over a channel* Γ, such that $\Gamma(i, j) = 1$ whenever $i \neq j$ (see [4]) . Let

$$w^\Gamma = \min\{\Gamma(i, j) : i \neq j\}, \qquad E^\Gamma = \{(j, k) : \Gamma(j, k) = w^\Gamma\} \tag{1}$$

and

$$L^\Gamma_\ell(k) = \{j : j \in \mathcal{Q},\, \Gamma(j, k) = \ell\} \quad \text{for each } k \in \mathcal{Q} \text{ and } 0 \leq \ell \leq e. \tag{2}$$

For any choice of the parameters q, e, M, and for any channel Γ, let $N^{[q]}(M, e)$ be the minimum number of questions that Paul must ask in order to determine a number $x_* \in \{0, 1, \ldots, M-1\}$, in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ, with total weight e. In this paper we deal with a dual version of this problem and we determine the largest possible $M = M(q, e, \Gamma, n)$ such that for all possible choices of the parameters q, e, n, and for any channel Γ, there exists a strategy of size n for Paul to determine a number $x_* \in \{0, 1, \ldots, M-1\}$ in the q-ary Rényi-Berlekamp-Ulam game with lies over the channel Γ with total weight e.

Related works The Rényi-Berlekamp-Ulam game was introduced independently in [12], [13] (in the realm of error-correcting codes for the noiseless delay-less feedback channel the same problem had been also considered in [2]). Since these seminal treatments many models of fault-tolerant search have been studied, see the surveys [8], [11], [9]. In [6] the issue of reducing adaptiveness in optimal search strategies tolerant against symmetric errors was first considered (see also [7,1]). A first step towards the study of the Rényi-Berlekamp-Ulam game over an arbitrary channel Γ as described here was taken in [10] and [4] where the authors considered the particular case of $\Gamma(i, j) \in \{1, e+1\}$ for all $i \neq j$.

In the context of the theory of error-correcting codes, our searching strategies are the same as shortened error-correcting codes for the noiseless delay-less feedback channel where a cost is incurred either for the transmission or the reception of a bit.

2 Searching with lies over a general channel

Before the game starts we fix three non-negative integers $q \geq 2$, $M \geq 1$ and $e \geq 0$, together with a channel Γ. Then the search space is identified with the set $\mathcal{U} = \{0, 1, \ldots, M-1\}$. The set of possible answers to a q-ary question is set to $\mathcal{Q} = \{0, 1, \ldots, q-1\}$. Carole chooses a number $x_* \in \mathcal{U}$ and Paul must guess it by asking as few q-ary questions as possible. Carole is allowed to choose wrong answers with total weight e on the channel Γ. We say that the current weight available to Carole is $e - w$ if the sum of the individual weights of her previous answers equals w. At any stage of the game, when questions $\mathbf{T}_1, \ldots, \mathbf{T}_t$ have been asked and answers $\mathbf{B}^t = b_1, \ldots, b_t$ have been received (with $b_i \in \mathcal{Q}$) Paul's *state* of knowledge is represented by an $(e+1)$-tuple $\sigma = (A_0, A_1, A_2, \ldots, A_e)$ of pairwise disjoint subsets of $\mathcal{U}$, where for each $i = 0, 1, 2, \ldots, e$ A_i is the set of elements of $\mathcal{U}$ which could possibly coincide with x_* supposing that the sum of the individual weights of Carole's answers $b_1, \ldots, b_t$ equals i. In particular, the *initial* state σ_0 is given by $(\mathcal{U}, \emptyset, \emptyset, \ldots, \emptyset)$. Let $k = b_t$ and assume Paul is in state $\sigma_{t-1} = (B_0, \ldots, B_e)$. Then Paul's new state $\sigma_t = \sigma_{t-1}^k = (C_0^k, \ldots, C_e^k)$ resulting from Carole's answer k to question $\mathbf{T}_t$ is given by

$$C_i^k = \bigcup_{\{j \in \mathcal{Q} \,:\, \Gamma(j,k) \leq i\}} \left(B_{i-\Gamma(j,k)} \cap T_j \right). \tag{3}$$

By induction, Carole's answers $b_1, \ldots, b_t$ determine a sequence of states

$$\sigma_0 = \sigma, \quad \sigma_1 = \sigma_0^{b_1}, \quad \sigma_2 = \sigma_1^{b_2}, \quad \ldots, \quad \sigma_t = \sigma_{t-1}^{b_t}.$$

A state $(A_0, A_1, A_2, \ldots, A_e)$ is *final* iff the set $A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_e$ has at most one element. By a *strategy $\mathcal{S}$ with n questions* we mean the q-ary tree of depth n, where each node ν is mapped into a question $\mathbf{T}_\nu$, and the q edges $\eta_0, \eta_1, \ldots, \eta_{q-1}$ generated by ν are, respectively from left to right, labeled with 0, 1, $\ldots, q-1$, which represent Carole's possible answers to $\mathbf{T}_\nu$. Let $\vec{\eta} = \eta_1, \ldots, \eta_n$ be a path in $\mathcal{S}$, from the root to a leaf, with respective labels $b_1, \ldots, b_n$, generating nodes $\nu_1, \ldots, \nu_n$ and associated questions $\mathbf{T}_{\nu_1}, \ldots, \mathbf{T}_{\nu_n}$. We say that strategy $\mathcal{S}$ is *winning* for σ iff for every path $\vec{\eta}$ the state $\sigma^{\vec{\eta}}$ is final. A strategy is said to be *nonadaptive* if all nodes at the same depth of the tree are mapped into the same question.

For a state $\sigma = (A_0, A_1, \ldots, A_e)$, we define the *type* of σ as the $(e+1)$-tuple whose ith coordinate coincides with the cardinality of A_i. We shall sometimes identify σ with its type and write $\sigma = (a_0, a_1, \ldots, a_e)$, where $a_i = |A_i|$, for each $i = 0, 1, \ldots, e$. Accordingly, for a question $\mathbf{T} = \{T_0, T_1, \ldots, T_{q-1}\}$, asked when the state is σ we define the type of $\mathbf{T}$ as the matrix

$$\Pi_{\mathbf{T}} = [t_{i,j}]_{0 \leq i \leq e,\, j \in \mathcal{Q}}$$

such that $t_{i,j} = |T_j \cap A_i|$. Then the type of Paul's new state, $\sigma^k = (b_0^k, \ldots, b_e^k)$ resulting from Carole's answer k to question $\mathbf{T}$ of type $\Pi_{\mathbf{T}}$ is given by

$$b_i^k = \sum_{\ell=0}^{i} \sum_{\{j \in \mathcal{Q} \,:\, \Gamma(j,k)=i-\ell\}} t_{\ell,j}. \tag{4}$$

3 An upper bound for the size of the search space

Using a result of [10] in this section we shall give an upper bound on the largest integer M such that Paul has a strategy of size n to determine Carole's secret number in the Rényi-Berlekamp-Ulam game over the channel Γ with total weight e, over a search space of cardinality M. Our result holds for any Γ with $\Gamma(i,i) = 0$ and $\Gamma(i,j) > 0$ for all i, j $(i \neq j)$, and for all sufficiently large n .

Theorem 1 [Dumitriu, Spencer]
Fix integers $q \geq 2$ and $e \geq 0$ and let $\mathcal{Q} = \{0, 1, \ldots, q-1\}$. Fix $\Gamma : \mathcal{Q} \times \mathcal{Q} \to \{0, 1, e+1\}$ such that $\Gamma(i,j) = 0$, iff $i = j$, for each $i, j \in \mathcal{Q}$. Let $E = \{(i,j) \in \mathcal{Q} \times \mathcal{Q} : \Gamma(i,j) = 1\}$. Then, for all $\epsilon > 0$ there exists an integer $n_0 > 0$ such that for all $n \geq n_0$, if Paul has a strategy of size n to determine a number $x_* \in \{0, 1, \ldots, M-1\}$ in the q-ary Rényi-Berlekamp-Ulam game with lies over the channel Γ, with total weight e, then

$$M \leq \left(\left(\frac{q}{|E|} \right)^e + \epsilon \right) \frac{q^n}{\binom{n}{e}}.$$

As a consequence, recalling the definition of w^Γ, and E^Γ in (1) we have:

Theorem 2 *Fix integers $q \geq 2$ and $e \geq 0$ and let $\mathcal{Q} = \{0, 1, \ldots, q-1\}$. Fix a function $\Gamma : \mathcal{Q} \times \mathcal{Q} \to \mathbb{N}_0$ such that $\Gamma(i,i) = 0$ for each i and $\Gamma(i,j) > 0$ for $i \neq j$. Then for all $\epsilon > 0$ there exists an integer n_0, such that for all integers $n > n_0$, if Paul has a strategy of size n to determine a number $x_* \in \{0, 1, \ldots, M-1\}$, in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ, with total weight e, then*

$$M \leq \left(\left(\frac{q}{|E^\Gamma|} \right)^{\lfloor \frac{e}{w^\Gamma} \rfloor} + \epsilon \right) \frac{q^n}{\binom{n}{\lfloor \frac{e}{w^\Gamma} \rfloor}}.$$

Proof. Let $\Gamma_1^U : \mathcal{Q} \times \mathcal{Q} \to \{0, w^\Gamma, e+1\}$ be defined by

$$\Gamma_1^U(i,j) = \begin{cases} \Gamma(i,j), \text{ if } \Gamma(i,j) \in \{0, w^\Gamma\} \\ e+1, \quad \text{otherwise.} \end{cases}$$

For any fixed M, e, n, if Paul has no winning strategy with n questions in a game over the channel Γ_1^U, then he has no winning strategy for the game over the channel Γ. In fact, over the channel Γ Carole can choose her lies more freely than over Γ_1^U, whence Paul's tasks can only

become more difficult. Moreover, in the game over Γ_1^U each one of Carole's lies weighs exactly w^Γ. Since the total weight of her lies cannot exceed e, the maximum number of her wrong answers is at most $\left\lfloor e/w^\Gamma \right\rfloor$. Let $\Gamma_2^U : \mathcal{Q} \times \mathcal{Q} \to \{0, 1, e+1\}$ be defined by

$$\Gamma_2^U(i,j) = \begin{cases} 1, & \text{if } \Gamma_1^U(i,j) = w^\Gamma \\ \Gamma_1^U(i,j), & \text{otherwise.} \end{cases}$$

Trivially, the game over Γ_1^U with total weight e is equivalent to the game over Γ_2^U with total weight $\left\lfloor e/w^\Gamma \right\rfloor$. Thus, for all $n = 1, 2, \ldots, ,$ we have

$$M(q, e, \Gamma, n) \leq M(q, e, \Gamma_1^U, n) = M(q, \lfloor e/w^\Gamma \rfloor, \Gamma_2^U, n).$$

Then from Theorem 1 we immediately get the desired conclusion. □

4 Optimal strategies for the game over a channel Γ

In the rest of the paper we shall prove the existence of a strategy which almost matches the bound given by Theorem 2. In fact, our upper and lower bounds match for all instances when e is a multiple of w^Γ.

Theorem 3 *Fix integers $e \geq 0$ and $q \geq 2$ and let $\mathcal{Q} = \{0, 1, \ldots, q-1\}$. Fix a function $\Gamma : \mathcal{Q} \times \mathcal{Q} \to \mathbb{N}_0$ satisfying $\Gamma(i,i) = 0$ for all $0 \leq i \leq q-1$. Then for all $\epsilon > 0$ there exists an integer n_0, such that for all integers $n > n_0$, if*

$$M \leq \left(\left(\frac{q}{|E^\Gamma|} \right)^{\left\lceil \frac{e}{w^\Gamma} \right\rceil} + \epsilon \right) \frac{q^n}{\binom{n}{\left\lceil \frac{e}{w^\Gamma} \right\rceil}}, \tag{5}$$

then Paul has a strategy of size n to determine a number $x_* \in \{0, 1, \ldots, M-1\}$, in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ, with total weight e.

4.1 The structure of the proof

We shall assume that the channel Γ has been fixed together with the parameters e, n, M satisfying (5). In order to ease the notation, we shall write $w, E, L_\ell(k)$ for $w^\Gamma, E^\Gamma, L_\ell^\Gamma(k)$, respectively.

We shall also use an additional parameter $\hat{e} = \lceil e/w \rceil w$, as described below.

We shall consider a modified game in which Carole has the possibility to use lies whose total weight is bounded by $\hat{e}$. Moreover, we shall assume that the game starts from a state which is worse (for Paul) than the official initial state $\sigma = (M, 0, \ldots, 0)$. We allow Carole to choose her secret number from a set of cardinality larger than M. This superset of the search space is

partitioned into $\hat{e}+1$ parts $S_0, S_1 \ldots, S_{\hat{e}}$, where $\mathcal{U} \subset S_0$. If Carole chooses the secret number from S_j then she agrees to answer in such a way that the total weight of her answers does not overcome $\hat{e}-j$.

For Paul this new setting is clearly worse than the original one. On the other hand because of its more symmetrical structure, such a state will allow us an easier description of the optimal strategy.

We shall also assume that the channel used to charge Carole's lies is the most difficult one (for Paul) among the channels over $\mathcal{Q} \times \mathcal{Q}$ which have minimum error transition cost equal to w and whose set of error transitions of minimum cost coincides with E. More precisely, we shall assume that Paul agrees to decrease to $w+1$ the charge for each of Carole's lies that has weight greater than w on the channel Γ.

Paul's strategy will consist of two phases. In the first phase Paul will ask $\mathcal{O}(\log M)$ *perfect questions*. These are questions that allow Paul to maximize the information gained from each of Carole's answers.

The second phase will consists of $n - \mathcal{O}(\log M)$ questions obtained via a well known procedure in the theory of error-correcting codes. This will imply that Paul can actually ask this final set of questions in a non-adaptive fashion. We shall first proceed to the analysis of the second phase and then complete the proof by showing that perfect questions can be used to reach the necessary conditions for the second phase to start.

The effectiveness of the perfect questions will be first shown for the special case when the channel belongs to the class of the d-rightregular channels introduced in [3]. This warm up will give us the possibility to show that for a d-rightregular channel a stronger version of Theorem 3 holds. In fact when the channel is d-rightregular the optimal strategies can be implemented as two batch procedures, i.e., as minimum adaptiveness algorithms.

4.2 Initial conditions - technicalities

The following results allow us to modify the parameters of the game for the purpose of the analysis and to consider a setting in which the initial state and the structure of the channel satisfy some useful symmetry requirements.

Lemma 1 (Dumitriu-Spencer) *For any $\alpha < \alpha' < \left(\frac{q}{|E|}\right)^{\frac{\hat{e}}{w}}$, there exist r and n_0 such that for any $n \geq n_0$ and for any $M < \alpha \frac{q^n}{\binom{n}{\frac{\hat{e}}{w}}}$, there exists a number aq^m with $a \in (q^r, q^{r+1}] \cap \mathbb{N}$ such that $M \leq aq^m < \alpha' \frac{q^n}{\binom{n}{\frac{\hat{e}}{w}}}$.*

Proposition 1 *Let the parameters e, q, Γ, M and n be as in Theorem 3. Let $\hat{e} = \lceil e/w \rceil w$ and a and m be given by Lemma 1. Let $c_0 = 1, c_1, \ldots, c_{\hat{e}}$ be non-negative integers. For each*

$i = 0, 1, \ldots, \hat{e}$, *let*

$$s_i = \begin{cases} q^{m-\lfloor \frac{i}{w} \rfloor}, \text{ if } \quad i \bmod w \leq \left\lfloor \frac{i}{w} \right\rfloor \\ 0, \qquad\quad \text{otherwise.} \end{cases}$$

If Paul has a winning strategy with n questions in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel

$$\Gamma'(i,j) = \begin{cases} \Gamma(i,j), \text{ if } \Gamma(i,j) \in \{0, w\} \\ w+1, \text{ otherwise.} \end{cases}$$

with total weight $\hat{e}$ starting from the state

$$\sigma_{IN} = (ac_0s_0,\, ac_1s_1,\, ac_2s_2,\, \ldots,\, ac_{\hat{e}}s_{\hat{e}}), \tag{6}$$

then Paul has a strategy of size n to determine a number $x_* \in \{0, 1, \ldots, M-1\}$, in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ, with total weight e.

Recalling the definition of $M(q, e, \Gamma, n)$ we have $M(q, e, \Gamma, n) \geq M(q, e, \Gamma', n) \geq M(q, \hat{e}, \Gamma', n)$. In fact, in the Rényi-Berlekamp-Ulam game over the channel Γ', with total weight e, each lie has a weight that cannot exceed the weight of a corresponding lie in the Rényi-Berlekamp-Ulam game over the channel Γ. Trivially, any winning strategy for the game over channel Γ' with total weight e is also a winning strategy for the game over channel Γ with total weight e. Moreover, any winning strategy for the game over channel Γ' with total weight $\hat{e}$ is also a winning strategy for the game over channel Γ' with total weight e, since in the former case we are giving Carole more freedom to lie. We shall prove that under the hypothesis (5), there is a strategy for Paul to determine a number in the set $\{0, 1, \ldots, aq^m - 1\}$ in the Rényi-Berlekamp-Ulam game over the channel Γ' with total weight $\hat{e}$. Theorem 3 will then follow from the chain of inequalities

$$M(q, e, \Gamma, n) \geq M(q, e, \Gamma', n) \geq M(q, \hat{e}, \Gamma', n) \geq aq^m \geq M. \tag{7}$$

Henceforth we shall assume that the channel Γ chosen by Paul and Carole coincides with the channel Γ' given by the above proposition. Therefore, there are exactly $|E|$ error transitions of cost w and $q^2 - q - |E|$ error transitions of cost $w + 1$.

Notice that, in the expanded game we are considering with total weight of lies $\hat{e}$, and minimum lie weight w we have that $\hat{e}/w$ is an integer and in particular it coincides with $\lceil e/w \rceil$.

To avoid repetitions, in the following we shall generally omit the quantification on the parameters $e, \hat{e}, q, M, n, w, a, \alpha, \alpha', m$ and tacitly assume, that they are as given in Theorem 3, Lemma 1 and Proposition 1.

5 The last $n - m + \frac{\hat{e}}{w}$ questions

We shall first describe the final part of Paul's strategy. This phase begins as soon as Paul reaches a state $\sigma = (A_0, A_1 \ldots, A_{\hat{e}})$ such that

$$|A_i| \leq a\, q^{\frac{\hat{e}}{w}} (q-1)^{\lfloor \frac{i}{w} \rfloor} \binom{m - \frac{\hat{e}}{w}}{\lfloor \frac{i}{w} \rfloor} + \mathcal{O}\left((m - \frac{\hat{e}}{w})^{\lfloor \frac{i}{w} \rfloor - 1} \right) \qquad \text{for } i = 0, 1, \ldots, \hat{e} - 1, \tag{8}$$

and

$$|A_{\hat{e}}| \leq a\, |E|^{\frac{\hat{e}}{w}} \binom{m - \frac{\hat{e}}{w}}{\frac{\hat{e}}{w}} + \mathcal{O}\left((m - \frac{\hat{e}}{w})^{\frac{\hat{e}}{w} - 1} \right). \tag{9}$$

Theorem 4 at the end of this section proves that once such a condition is fulfilled, Paul can easily get through to an easy and successful end of the game by using at most $n - m + \frac{\hat{e}}{w}$ additional questions. [2]

We shall need the following technical lemmas.

Lemma 2 *Let $A_0, A_1, \ldots, A_{\hat{e}}$ satisfy (8)-(9), then there exists a n_0 such that for all $n \geq n_0$ we have the inequality*

$$q^{n-m+\frac{\hat{e}}{w}} \geq \left(\sum_{j=0}^{\hat{e}-1} |A_j| \right) \left(\sum_{i=0}^{2\hat{e}/w} \binom{n - m + \frac{\hat{e}}{w}}{i} q^i \right) + |A_{\hat{e}}|. \tag{10}$$

Proof.

First we notice that by Lemma 1 we have

$$m \leq n - \log_q \left(\binom{n}{\frac{\hat{e}}{w}} \frac{a}{\alpha'} \right). \tag{11}$$

The desired result is a direct consequence of the following two claims.

Claim 1. The following inequality holds:

$$m \leq \left(\frac{\alpha' \frac{\hat{e}}{w}!\, q^{n-m}}{a} \right)^{\frac{1}{\frac{\hat{e}}{w}}} + \frac{\hat{e}}{w}. \tag{12}$$

For otherwise (absurdum hypothesis) we would have

[2] Therefore, in order to complete the proof of Theorem 3 it will be enough to show that a state fulfilling (8)-(9) can be reached within the first $m - \frac{\hat{e}}{w}$ questions. This part is deferred to the next sections.

$$\binom{n}{\frac{\hat{e}}{w}}\frac{a}{\alpha'} > \binom{m}{\frac{\hat{e}}{w}}\frac{a}{\alpha'} \geq \frac{\left(m-\frac{\hat{e}}{w}\right)^{\frac{\hat{e}}{w}}}{\frac{\hat{e}}{w}!}\frac{a}{\alpha'} \geq \frac{\left(\left(\frac{\alpha'\frac{\hat{e}}{w}!\,q^{n-m}}{a}\right)^{\frac{1}{\frac{\hat{e}}{w}}}\right)^{\frac{\hat{e}}{w}}}{\frac{\hat{e}}{w}!}\frac{a}{\alpha'} = q^{n-m}$$

contradicting (11). Our first claim is settled.

Claim 2. There exists a constant $0 < \gamma < 1 - \alpha' \left(\frac{|E|}{q}\right)^{-\frac{\hat{e}}{w}}$, such that

$$|A_{\hat{e}}| \leq (1-\gamma) q^{n-m+\frac{\hat{e}}{w}} \tag{13}$$

We have the following for $n \geq n_0$:

$$\begin{aligned}
|A_{\hat{e}}| &\leq |E|^{\frac{\hat{e}}{w}} \binom{m-\frac{\hat{e}}{w}}{\hat{e}/w} a + \mathcal{O}\left((m-\frac{\hat{e}}{w})^{\frac{\hat{e}}{w}-1}\right) && (14)\\
&\leq |E|^{\frac{\hat{e}}{w}} \binom{n}{\hat{e}/w} a && (15)\\
&\leq \alpha'\, q^{n-m}\, |E|^{\frac{\hat{e}}{w}} && (16)\\
&\leq (1-\gamma) q^{n-m+\frac{\hat{e}}{w}}. && (17)
\end{aligned}$$

where

- (14) directly follows from (9),
- (15) follows from e, w constant, (11) and the properties of the binomial coefficient,
- (16) follows from (11),
- (17) follows from the fact that $\alpha' < \left(\frac{|E|}{q}\right)^{-\frac{\hat{e}}{w}}$.

This settles our second claim.

We are now ready to complete the proof of the lemma. By (8), we have that there exist polynomials $\mathbf{p}$ and $\mathbf{p}_1$, such that

$$\begin{aligned}
&|A_{\hat{e}}| + \left(\sum_{j=0}^{\hat{e}-1} |A_j|\right)\left(\sum_{i=0}^{2\hat{e}/w} \binom{n-m+\frac{\hat{e}}{w}}{i} q^i\right)\\
&\quad < (\hat{e}-1)\left(\max_{0\leq j\leq \hat{e}-1} |A_j|\right)\left(\sum_{i=0}^{2\hat{e}/w} \binom{n-m+\frac{\hat{e}}{w}}{i} q^i\right) + (1-\gamma) q^{n-m+\frac{\hat{e}}{w}} && (18)\\
&\quad \leq \binom{m-\frac{\hat{e}}{w}}{\frac{\hat{e}}{w}-1} \mathbf{p}(n-m+\frac{\hat{e}}{w}) + (1-\gamma) q^{n-m+\frac{\hat{e}}{w}} && (19)
\end{aligned}$$

$$\leq \frac{\left(\left(\frac{\alpha' \frac{\hat{e}}{w}! \, q^{n-m}}{a}\right)^{\frac{1}{\frac{\hat{e}}{w}}}\right)^{\frac{\hat{e}}{w}-1}}{(\frac{\hat{e}}{w}-1)!}\mathbf{p}(n-m+\frac{\hat{e}}{w}) + (1-\gamma)q^{n-m+\frac{\hat{e}}{w}} \tag{20}$$

$$\leq \mathbf{p}_1(n-m)q^{(n-m)\frac{\frac{\hat{e}}{w}-1}{\frac{\hat{e}}{w}}} + (1-\gamma)q^{n-m+\frac{\hat{e}}{w}} \tag{21}$$

$$< \gamma q^{n-m+\frac{\hat{e}}{w}} + (1-\gamma)q^{n-m+\frac{\hat{e}}{w}}. \tag{22}$$

Here,

- (18) follows by the sizes of the sets A_i being monotonically increasing and by Claim 2,
- (19) follows from (8), upon noting that

$$\max_{0\leq j\leq \hat{e}-1} |A_j| \leq a\, q^{\frac{\hat{e}}{w}}(q-1)^{\frac{\hat{e}}{w}-1}\binom{m-\frac{\hat{e}}{w}}{\frac{\hat{e}}{w}-1} + \mathcal{O}\left((m-\frac{\hat{e}}{w})^{\frac{\hat{e}}{w}-2}\right)$$

  and in the asymptotics analysis employed here,

$$(\hat{e}-1)q^{\hat{e}/w}(q-1)^{\frac{\hat{e}}{w}-1}a\left(\sum_{i=0}^{2\hat{e}/w}\binom{n-m+\frac{\hat{e}}{w}}{i}q^i\right)$$

  and the term in the $\mathcal{O}$ notation can be absorbed in a multiplicative factor as a polynomial in $(n-m+\frac{\hat{e}}{w})$,
- (20) trivially follows from (12) and the properties of the binomial coefficient,
- (21) follows because $\frac{\mathbf{p}(n-m+\frac{\hat{e}}{w})\left(\frac{\alpha' \frac{\hat{e}}{w}!}{a}\right)^{1-\frac{1}{\frac{\hat{e}}{w}}}}{(\frac{\hat{e}}{w}-1)!}$ is bounded by a polynomial in $n-m$ of degree $2\frac{\hat{e}}{w}$,
- (22) holds for all $n > m-\left(\frac{\hat{e}}{w}\right)^2+\frac{\hat{e}}{w}\log_q\frac{\mathbf{p}_1(n-m)}{\gamma}$, since the exponent of q in $\mathbf{p}_1(n-m)q^{(n-m)\frac{\frac{\hat{e}}{w}-1}{\frac{\hat{e}}{w}}}$ is smaller than $n-m+\frac{\hat{e}}{w}$

The proof is complete. □

Lemma 3 *Let $A_0, A_1, \ldots, A_{\hat{e}}$ satisfy (8)-(9). Then there exist disjoint sets, $\mathcal{C}_1, \mathcal{C}_2$, of q-ary tuples of length $n-m+\frac{\hat{e}}{w}$ such that*

(i) $|\mathcal{C}_1| \geq \sum_{i=0}^{\hat{e}-1}|A_i|$,
(ii) *for all* $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}_1$, $d_H(\mathbf{x}_1, \mathbf{x}_2) \geq 2\frac{\hat{e}}{w}+1$,
(iii) $|\mathcal{C}_2| \geq |A_{\hat{e}}|$,
(iv) *for all* $\mathbf{x}_1 \in \mathcal{C}_1, \mathbf{x}_2 \in \mathcal{C}_2$, $d_H(\mathbf{x}_1, \mathbf{x}_2) \geq \frac{\hat{e}}{w}+1$,

where $d_H(\cdot,\cdot)$ denotes Hamming distance between q-ary vectors.

Proof. The sets $\mathcal{C}_1$ and $\mathcal{C}_2$ will be constructed via the following greedy algorithm [3]. Let $\mathcal{R} = \{0,1,\ldots,q-1\}^{n-m+\frac{\hat{e}}{w}}$. We first build the set $\mathcal{C}_1 \subseteq \mathcal{R}$ by the following procedure:

[3] This algorithm is an *ad hoc* version of the well known Gilbert procedure.

1. Pick an arbitrary vector $\mathbf{x} \in \mathcal{R}$ and include it in $\mathcal{C}_1$.
2. Delete from $\mathcal{R}$ all vectors $\mathbf{y}$ such that $d_H(\mathbf{x}, \mathbf{y}) \leq 2\frac{\hat{e}}{w}$.
3. If $|\mathcal{C}_1| \leq \sum_{i=0}^{\hat{e}-1} |A_i|$ go back to 1.

Direct inspection shows that each time step 2. is performed, at most $\sum_{j=0}^{2\hat{e}/w} \binom{n-m+\frac{\hat{e}}{w}}{j} q^j$ vectors are deleted from $\mathcal{R}$. Lemma 2 guarantees that, as long as $|\mathcal{C}_1'| \leq \sum_{i=0}^{\hat{e}-1} |A_i|$, one can add new elements to $\mathcal{C}_1'$: indeed, there are more elements in the set $\{0, 1, \ldots, q-1\}^{n-m+\frac{\hat{e}}{w}}$ than in the union of $\mathcal{C}_1'$ and the set of deleted vectors. Once the set $\mathcal{C}_1$ has been constructed with its $\sum_{i=0}^{\hat{e}-1} |A_i|$ vectors, by Lemma 2 in $\mathcal{R} \setminus \mathcal{C}_1$ there still exist $|A_{\hat{e}}|$ many vectors which have not been discarded during the construction of $\mathcal{C}_1$. These vectors will constitute the set $\mathcal{C}_2$. By direct inspection, $\mathcal{C}_1$ and $\mathcal{C}_2$ satisfy (ii) and (iv). The proof is complete. □

Theorem 4 *Let $A_0, A_1, \ldots, A_{\hat{e}}$ satisfy (8)-(9). Then, starting from the state $\sigma = (A_0, A_1, \ldots, A_{\hat{e}})$ Paul has a non-adaptive winning strategy of size $n - m + \frac{\hat{e}}{w}$ in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ', with total weight $\hat{e}$.*

Proof. We shall show that starting from the state σ, a batch of $n-m+\frac{\hat{e}}{w}$ nonadaptive questions is sufficient to guess the secret number x_* in the Rényi-Berlekamp-Ulam game over the channel Γ' with total weight e.

Let the encoding function θ send all elements of $\cup_{j=0}^{\hat{e}-1} A_j$ one-to-one onto q-ary tuples in $\mathcal{C}_1$, and all elements of $A_{\hat{e}}$ one-to-one onto q-ary tuples in $\mathcal{C}_2$. Let $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ be the range of θ. Paul will ask his batch of questions with the aim of guessing the encoding $\mathbf{x}_*^\theta \in \mathcal{C}$ of Carole's secret number x_*. Our constraints on the Hamming distance between any two q-tuples in $\mathcal{C}_1$ and $\mathcal{C}_2$ are just to ensure that Paul will be able to identify x_*, no matter Carole's wrong answers. As a matter of fact, there are two possible cases:

Case 1. The secret number x_* is an element of $\cup_{j=0}^{\hat{e}-1} A_j$. Then Carole can give at most $\hat{e}/w$ wrong answers. Any tuple $\mathbf{x} \in \mathcal{C}$ representing a number $\neq x_*$ will differ from $\mathbf{x}_*^\theta$ in at least $2\hat{e}/w + 1$ digits. From the tuple $\mathbf{a}$ of Carole's answers, Paul will correctly guess x_*, as the only possible number corresponding to the tuple in $\mathcal{C}$ having minimum distance from $\mathbf{a}$.

Case 2. The secret number belongs to $A_{\hat{e}}$. Then Carole must give correct answers to all remaining questions. As a matter of fact, each lie weighs at least w and, under our standing hypothesis for this case, Carole's available weight is less then w. Carole's answers will necessarily coincide with the encoding x_*^θ of x_*. Again, by choosing the tuple of $\mathcal{C}$ which is closest to the tuple of Carole's answers, Paul will correctly guess the secret number. In either case Paul must only find the tuple in $\mathcal{C}$ which is closest to the tuple of Carole's answers. This tuple does correspond to Carole's secret number x_*.

The proof is now complete. □

6 The first $m - \frac{\hat{e}}{w}$ questions

Perfect questions

The first phase of Paul's strategy relies on the existence of the so called Perfect Questions.

Definition 1 (Perfect questions) *A question* $\mathbf{T}$ *is* perfect *for a state* $\sigma = (x_0, x_1, \ldots, x_{\hat{e}})$ *if there exists a state* $\sigma_{Next} = (y_0, y_1, \ldots, y_{\hat{e}})$*, such that, when Paul is in the state* σ *and asks question* $\mathbf{T}$ *then for each* $k = 0, 1, \ldots, q-1$*, the state resulting form Carole's answer* k *coincides with* σ_{Next}*.*

Perfect questions play a central role in our strategies because they balance at the best the information content among all of Carole's possible answers. A perfect question is not prone to an adversary strategy. As long as Paul is able to ask perfect questions Carole has no room for trying to implement a devil's strategy. Since each possible answer (a correct one or a lie) of Carole's leads to the "same state" [4] the dynamics of Paul's states (of knowledge) is predetermined.

The problem in trying to use perfect questions is that they may not exist for the state under consideration. In fact, the key point in our argument is to show that perfect questions are available to Paul until the game reaches the conditions for the start of the final stage.

Fact 1 *Given a state* $\sigma = (x_0, x_1, \ldots, x_{\hat{e}})$*, a question* $\mathbf{T}$ *of type* $\Pi_{\mathbf{T}} = [t_{i,j}]$ *is perfect for* σ *if the following conditions are satisfied*

$$x_i = \sum_{j=0}^{q-1} t_{ij} \tag{23}$$

$$x_i^k = t_{i,k} + \sum_{\ell \in L_w(k)} t_{i-w,\ell} + \sum_{\ell \in L_{w+1}(k)} t_{i-w-1,\ell} \quad \textit{for each } j = 0, 1, \ldots, \hat{e} \tag{24}$$

for each $i = 0, 1, \ldots, \hat{e}$ *and* $k = 0, 1, \ldots, q-1$*, where* $\sigma^k = (x_0^k, \ldots, x_{\hat{e}}^k)$ *is the state resulting from Carole's answer* k*.*

The system of equations (23)-(24) has the following solution:

$$x_i^k = \frac{1}{q}\left(x_i + \sum_{j=0}^{q-1}\left(\sum_{\ell \in L_w(j)} t_{i-w,\ell} + \sum_{\ell \in L_{w+1}(j)} t_{i-w-1,\ell}\right)\right) \tag{25}$$

$$t_{i,k} = x_i^k - \sum_{\ell \in L_w(k)} t_{i-w,\ell} - \sum_{\ell \in L_{w+1}(k)} t_{i-w-1,\ell} \quad \text{for each } k = 0, 1, \ldots, \hat{e} \tag{26}$$

Unfortunately, equation (26) does not always define a feasible question since it might be the case that not all the question's components $t_{i,k}$'s and the next state's components x_i^k's as given by (25) are non-negative integers.

[4] In actual fact, different answers lead to different states but of the same type.

6.1 Warm up: d-rightregular channels

As a warm up we shall concentrate on the special case when the channel is d-rightregular [3].

Definition 2 [3] A channel Γ is said to be *d-rightregular*, if $|\{(j,k) : \Gamma(j,k) = w^\Gamma\}| = d$ for all $k \in \mathcal{Q}$.

Trivially, for a d-rightregular channel Γ, it holds that $d = |E|/q$. We shall start by proving a variant of Theorem 3 for the special case when Γ is a d-rightregular channel. The result restricted to this weaker variant of the game will be stronger. In fact, for the case of d-rightregular channels we shall prove that optimal strategies exist which are implementable with minimum adaptiveness, i.e., in two batches of non-adaptive questions.

Proposition 2 *Let $\sigma = (x_0, \ldots, x_e)$ in the q-ary Rényi-Berlekamp-Ulam game with lies, over the channel Γ, with total weight e. Let Γ be d-rightregular and x_i/q be an integer for each $i = 0, 1, \ldots, \hat{e}$.*

Then the question $\mathbf{T}$ of type $\Pi_{\mathbf{T}} = [t_{i,j}]$, defined by $t_{i,j} = x_i/q$, for each $j = 0, 1, \ldots, q-1$ and $i = 0, 1, \ldots, \hat{e}$, is perfect for the state σ. Moreover, let $\sigma^k = (y_0^k, y_1^k, \ldots, y_{\hat{e}}^k)$ be the state resulting from Carole's answer k. It holds that

$$y_i^k = \frac{1}{q}x_i + \frac{d}{q}x_{i-w} + \frac{q-1-d}{q}x_{i-w-1} = \frac{1}{q}\left(x_i + dx_{i-w} + (q-1-d)x_{i-w-1}\right). \tag{27}$$

Proof. The desired follows from Fact 1 and the definition of a d-rightregular channel that gives $|L_w(j)| = d$ and $L_{w+1}(j) = q-1-d$ for each $j = 0, 1, \ldots, q-1$. □

Recall the definition of the initial state $\sigma_{IN} = (ac_0s_0,\ ac_1s_1,\ ac_2s_2,\ \ldots,\ ac_{\hat{e}}s_{\hat{e}})$, given in Proposition 1, where $c_0, \ldots, c_{\hat{e}}$ are non-negative integers to be determined.

Let us fix $c_0 = 1$. Therefore, if Γ is a d-rightregular channel for any choice [5] of non-negative integers $c_1, c_2, \ldots, c_{\hat{e}}$, iterated application of the above proposition shows that Paul can ask $m - \frac{\hat{e}}{w}$ perfect questions.

Note that after the $\left(m - \frac{\hat{e}}{w}\right)$th question has been answered, the state resulting from Carole's answer might have the last component which is not a multiple of a power of q anymore. Hence Paul cannot count on perfect questions in the remaining part of the game and will have to use a different strategy. As a matter of fact at that point, as we shall show, Paul will be in the position to start the final phase and successfully end the game within the next $n - m + \frac{\hat{e}}{w}$ questions.

[5] Actually for our present purposes it is enough to set $c_i = 0$ for each $i = 1, 2, \ldots, \hat{e}$.

6.1.1 Perfect questions are non-adaptive for the d-rightregular channel

It remarkable that the set of $m - \frac{\hat{e}}{w}$ questions described above can actually be implemented as a batch of non-adaptive questions. This can be done as follows. Let $\sigma = (S_0, S_1, \ldots, S_{\hat{e}})$ be the initial state of type $(ac_0s_0,\, ac_1s_1,\, ac_2s_2,\, \ldots,\, ac_{\hat{e}}s_{\hat{e}})$, as defined above. Let $f : x \in \bigcup_{i=0}^{\hat{e}} S_i \mapsto \mathbb{N}$ be a one-to-one function which sends each element of S_i into a number in $\left[\sum_{j=0}^{i-1} ac_js_j, \sum_{j=0}^{i} ac_js_j - 1\right] \cap \mathbb{N}$. *The first batch of questions* is defined as follows: For each $j = 1, 2, \ldots, m - \frac{\hat{e}}{w}$, let $\mathcal{D}_j = (D_{j\,0}, D_{j\,1}, \ldots, D_{j\,q-1})$ denote the question

- "What is the jth least-significant (q-ary) digit of $f(x_*)$?"

More precisely, a number $y \in \cup_{\ell=0}^{\hat{e}} S_\ell$ belongs to $D_{j\,i}$ iff the jth least significant digit y_j of the q-ary expansion of its image via $f(\cdot)$, $\mathbf{y} = y_1 \cdots y_m$ is equal to i. Let $b_j \in \{0, 1, \ldots, q-1\}$ be the answer to question $\mathcal{D}_i$. Let $\mathbf{B} = b_1 \cdots b_m$. Starting from the initial state $\sigma = (S_0, S_1, \ldots, S_{\hat{e}})$, Paul's state resulting from Carole's answers $b_1 \cdots b_m$ is the $(\hat{e}+1)$-tuple $\sigma^{\mathbf{B}} = (A_0, A_1, \ldots, A_{\hat{e}})$, where for all $i = 0, 1, \ldots, \hat{e}$, $A_i = \bigcup_{\ell=0}^{i} \{y \in S_\ell \mid d_{\Gamma'}(\mathbf{y}, \mathbf{B}) = i - \ell\}$ and $d_{\Gamma'}(\mathbf{y}, \mathbf{B}) = \sum_{i=1}^{m} \Gamma'(y_i, b_i)$. Therefore, for each $i = 0, 1, \ldots, \hat{e}$ and $\ell = 0, 1, \ldots, i$, a number y which was initially in S_ℓ will be eventually in A_i iff:

- There exists an integer $j \in \{0, 1, \ldots, \lfloor (i-\ell)/w \rfloor\}$ such that $(i - \ell - jw)/(w+1)$ is also an integer, and there exist two disjoint subsets of $\{1, 2, \ldots, m - \frac{\hat{e}}{w}\}$, say $W = \{k_1, k_2, \ldots, k_j\}$ and $W' = \{o_1, o_2, \ldots, o_{(i-\ell-wj)/(w+1)}\}$, such that

$$\Gamma'(y_u, b_u) = \begin{cases} w, & \text{if } u \in W \\ w+1, & \text{if } u \in W' \\ 0, & \text{otherwise.} \end{cases}$$

Thus,

$$|A_i| = \sum_{\ell=0}^{i} \left(\sum_{j=0}^{\lfloor \frac{i-\ell}{w} \rfloor} \binom{m - \frac{\hat{e}}{w}}{j} g(m - \frac{\hat{e}}{w} - j, \frac{i-\ell-jw}{w+1})(q-1-d)^{\frac{i-\ell-jw}{w+1}} d^j \right) ac_\ell \frac{s_\ell}{q^{m-\frac{\hat{e}}{w}}}, \qquad (28)$$

where

$$g(x, y) = \begin{cases} \binom{x}{y}, & \text{if } x, y \in \mathbb{N}_0 \\ 0, & \text{otherwise.} \end{cases}$$

Let us first consider the case $i = \hat{e}$. Recalling that $\hat{e}$ is divisible by w it is not hard to see that in (28) the asymptotically leading term is the one given by $\ell = 0$, $j = \lfloor \frac{i}{w} \rfloor$. Recalling that $c_0 = 1$, and that for d-regular channels $|E| = dq$ we have that for all sufficiently large m,

$$|A_{\hat{e}}| \leq \left(\binom{m - \frac{\hat{e}}{w}}{\frac{\hat{e}}{w}} d^{\frac{\hat{e}}{w}} + \mathcal{O}\left((m - \frac{\hat{e}}{w})^{\frac{\hat{e}}{w}-1} \right) \right) q^{\frac{\hat{e}}{w}} a$$

$$\leq |E|^{\frac{\hat{e}}{w}} \binom{m - \frac{\hat{e}}{w}}{\hat{e}/w} a + \mathcal{O}\left((m - \frac{\hat{e}}{w})^{\frac{\hat{e}}{w}-1} \right).$$

Moreover, by analogous argument and $d \leq q-1$, it is not hard to see that the following looser bound holds for each $i = 0, 1, \ldots, \hat{e} - 1$

$$|A_i| \leq \left(\binom{m - \frac{\hat{e}}{w}}{\lfloor \frac{i}{w} \rfloor} (q-1)^{\lfloor \frac{i}{w} \rfloor} + \mathcal{O}\left((m - \frac{\hat{e}}{w})^{\lfloor \frac{i}{w} \rfloor - 1} \right) \right) q^{\frac{\hat{e}}{w}} a$$

Therefore, after this batch of questions Paul's state satisfies (8)-(9).

Together with Theorem 2 the results in Sections 6.1 and 5 provide the following result for the Rényi-Berlekamp-Ulam game over a d-rightregular channel.

Theorem 5 *Fix integers $e \geq 0$ and $q \geq 2$ and let $\mathcal{Q} = \{0, 1, \ldots, q-1\}$. Fix an integer $0 \leq d \leq q-1$ and a d-rightregular channel Γ.*

Then,

$$M(q, e, \Gamma, n) \geq q^n \frac{d^{-\lceil \frac{e}{w} \rceil}}{\binom{n}{\lceil \frac{e}{w} \rceil}} (1 + o(1)),$$

and this bound is asymptotically tight in all cases where e is a multiple of w^Γ. Moreover the strategies attaining the above bound can be implemented with minimum adaptiveness, i.e., in two batches of nonadaptive questions.

6.2 From d-rightregular channels to arbitrary channels

In the previous section we have shown how Paul can implement the idea of perfect questions on a d-rightregular channel to obtain a two batch strategy that attain the bound in Theorem 3. In particular, such strategy is optimal whenever the minimum lie weight divides e.

In this section we shall need a slightly more involved machinery to show that we can extend the upper bound of the previous section to the case of non-regular channels, at the cost of losing the non-adaptiveness of the questions of the first stage. Notwithstanding the impossibility to count on the symmetric structure of the channel we shall show that asymptotically (with n) a non-regular channel Γ behaves "like" an $\frac{|E|}{q}$-rightregular channel.

By virtue of Proposition 1 and Theorem 4 in order to prove Theorem 3 it is enough to show that there are constants $c_0 = 1, c_1, \ldots, c_{\hat{e}}$, such that for all sufficiently large m starting in the

state σ_{IN} Paul can [6] ask $m - \frac{\hat{e}}{w}$ perfect questions as defined in (25)-(26) and the resulting state $(A_0, \ldots, A_{\hat{e}})$ satisfies (8).

For $u = 0, 1, \ldots$, let $\sigma^{(u)} = (A_0^{(u)}, A_1^{(u)}, \ldots, A_{\hat{e}}^{(u)})$ be the state of knowledge of Paul after the answer to the u-th question. In particular $\sigma^{(0)}$ coincides with σ_{IN}. Let $F = (\mathcal{Q} \times \mathcal{Q}) \setminus E$. Then, in particular, $|F| = q^2 - q - |E|$. We shall prove our claim by induction. The key observation is that the cardinality $|A_i^{(u)}|$ of the i-th component of the state of knowledge of Paul after u questions/answers satisfies the following.

(i) $|A_i^{(u)}|$ can be expressed as $a \cdot z_i(u) \cdot q^{m - \lfloor \frac{i}{w} \rfloor - u}$.
(ii) The coefficient $z_i(u)$ is a linear combination of $z_0(u-1), \ldots, z_i(u-1)$, with the coefficient of $z_i(u-1), z_{i-w}(u-1), z_{i-w-1}(u-1)$ being respectively $1, |E|$ and $|F|$, and the coefficients of $z_j(u-1)$ being 0 for $j = i - w + 1, \ldots, i - 1$.

Note that (i)-(ii) formalize the intuition that the recurrence governing the evolution of $|A_i^{(u)}|$ with respect to $\sigma^{(u-1)}$ cannot diverge much from (27).

Indeed, the next key observation will be that solving such recurrence $z_i(u)$ can be expressed as a linear combination of $c_0, c_1, \ldots, c_i$, whose coefficients are polynomials of u. In symbols, $z_i(u) = \sum_{j=0}^{i} p_{i,j}(u) \times c_j$, where for each $j = 0, 1, \ldots, i$, $p_{i,j}(u)$ is a polynomial in u. In particular, $p_{i,j}$ is asymptotically bounded by

$$|E|^{\lfloor \frac{i-j}{w} \rfloor} \binom{u}{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1}),$$

for all i divisible by w. In the remaining cases, $p_{i,j}$ can be asymptotically bounded by

$$(q \times (q-1))^{\lfloor \frac{i-j}{w} \rfloor} \binom{u}{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1}).$$

Lemma 4 *There exist constants $c_0 = 1, c_1, c_2, \ldots, c_{\hat{e}}$, and questions $\mathbf{T}_1, \ldots \mathbf{T}_{m - \frac{\hat{e}}{w}}$, such that for each $u = 1, 2, \ldots, m - \frac{\hat{e}}{w}$ we have*

$$|A_i^{(u)}| = \begin{cases} a q^{m - \lfloor \frac{i}{w} \rfloor - u} \sum_{j=0}^{i} c_j \left(|E|^{\lfloor \frac{i-j}{w} \rfloor} \binom{u}{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1}) \right) & \text{if } w | i, \\ a q^{m - \lfloor \frac{i}{w} \rfloor - u} \sum_{j=0}^{i} c_j \left((q \times (q-1))^{\lfloor \frac{i-j}{w} \rfloor} \binom{u}{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1}) \right) & \text{otherwise.} \end{cases}$$

Proof. For sake of definiteness let us set $t_{ik}^{(0)} = 0$ for each $i = 0, 1, \ldots, \hat{e}$ and each $k = 0, 1, \ldots, q-1$ and for $i = -(w+1), -w, \ldots, -1$, and for all $u = 0, 1, \ldots$, $|A_i^{(u)}| = 0$.

We shall first show that the validity of the bound on the components of the states of knowledge of Paul when he chooses his questions according to the rules in (25)-(26). Then we shall prove that constants $c_0, \ldots, c_{\hat{e}}$ exist that allow such questions, i.e., they guarantee that the questions defined by (25)-(26) are feasible since they satisfy the integrality and non-negativity constraints.

[6] Of course by can we mean that such questions are feasible, i.e., they satisfy the constraints of integrality and non-negativity together with the states they lead to.

The following claims are not difficult to prove by induction on i and u.

Claim 3. For each $u = 0, 1, \ldots$ and $i = 0, 1, \ldots, \hat{e}$, and $k = 0, 1, \ldots, q-1$, there exist integers $d_i^{(u)}$ and $\tau_{i\,k}^{(u)}$ such that $|A_i^{(u)}|/a = d_i^{(u)} q^{m-\lfloor \frac{i}{w} \rfloor - u}$ and $t_{i\,k}^{(u)} = \tau_{i\,k}^{(u)} q^{m-\lfloor \frac{i}{w} \rfloor - u}$.

The claim is obviously true when $u = 0$. Moreover, it is also easy to see that it holds when $i = 0$ for all $u > 0$, since $|A_0^{(u)}|/a = c_0 q^{m-u} = t_{0\,k}^{(u)}$, for all $k = 0, 1, \ldots, q-1$.

Now fix $u \geq 1$ and $i \in \{1, \ldots, \hat{e}\}$ and assume that the claim holds for all $A_{i'}^{(t')}$, such that either $t' < t$ or $t' = t$ and $i' < i$. Then we have

$$|A_i^{(u)}|/a = d_i^{(u-1)} q^{m-\lfloor \frac{i}{w} \rfloor - u} + \left(\sum_{j=0}^{q-1} \sum_{\ell \in L_w(j)} \tau_{i-w\,\ell}^{(u)} \right) q^{m-\lfloor \frac{i}{w} \rfloor - u} + \left(\sum_{j=0}^{q-1} \sum_{\ell \in L_{w+1}(j)} \tau_{i-w-1\,\ell}^{(u)} \right) q^{m-\lfloor \frac{i-1}{w} \rfloor - u}$$

and hence setting

$$d_i^{(u)} = d_i^{(u-1)} + \sum_{j=0}^{q-1} \sum_{\ell \in L_w(j)} \tau_{i-w\,\ell}^{(u)} + q^{\lfloor \frac{i}{w} \rfloor - \lfloor \frac{i-1}{w} \rfloor} \sum_{j=0}^{q-1} \sum_{\ell \in L_{w+1}(j)} \tau_{i-w-1\,\ell}^{(u)} \tag{29}$$

we have the desired result for the cardinality of $A_i^{(u)}$. Moreover by induction hypothesis we have

$$t_{i\,k}^{(u)} = d_i^{(u)} q^{m-\lfloor \frac{i}{w} \rfloor - u} - \sum_{\ell \in L_w(k)} \tau_{i-w\,\ell}^{(u)} q^{m-\lfloor \frac{i}{w} \rfloor + 1 - u} - \sum_{\ell \in L_{w+1}(k)} \tau_{i-w-1\,\ell}^{(u)} q^{m-\lfloor \frac{i-1}{w} \rfloor + 1 - u} \tag{30}$$

which proves the second part of the induction step with

$$\tau_{i\,k}^{(u)} = d_i^{(u)} - q \sum_{\ell \in L_w(k)} \tau_{i-w\,\ell}^{(u)} - q^{1+\lfloor \frac{i}{w} \rfloor - \lfloor \frac{i-1}{w} \rfloor} \sum_{\ell \in L_{w+1}(k)} \tau_{i-w-1\,\ell}^{(u)}. \tag{31}$$

Claim 4. For each $u = 1, 2, \ldots$ and $i = 0, 1, \ldots, q-1$, it holds that $d_i^{(u)} = \sum_{j=0}^{i} \delta_{i\,j} d_j^{(u-1)}$ with $\delta_{i\,j}$ integers and in particular $\delta_{i\,i} = 1, \delta_{i\,i-w} = |E|, \delta_{i\,i-w-1} = q^{\lfloor \frac{i}{w} \rfloor - \lfloor \frac{i-1}{w} \rfloor} |F|$, and $\delta_{i\,j} = 0$, for $j = i-w+1, i-w+2, \ldots, i-1$.

For $u = 0$, the claim is true for all $i = 0, 1, \ldots, \hat{e}$. Moreover, for $i = 0$, the claim is trivially true for all integer $u = 1, \ldots$.

Now fix $u \geq 1$ and assume that the claim is true for $i = 0, 1, \ldots, i'-1$. As an immediate consequence, using (29)-(31) we have that for all $i = 0, 1, \ldots, i'-1$ and for each $k = 0, 1, \ldots, q-1$, $\tau_{i\,k}^{(u)}$ is a linear combination of $\{d_j^{(u-1)} \mid j = 0, 1, \ldots, i\}$ with the coefficient of $d_i^{(u-1)}$ being 1. Then, the desired result directly follows from (29). Thus, writing $\tau_{i\,k} = \sum_{j=0}^{i} s_{k\,j} \times d_j^{(u-1)}$ and q_i' for $q^{\lfloor \frac{i}{w} \rfloor - \lfloor \frac{i-1}{w} \rfloor}$ we have $s_{k\,i} = 1$, for each k, whence

$$
\begin{aligned}
d_i^{(u)} &= d_i^{(u-1)} + \sum_{j=0}^{q-1} \sum_{\ell \in L_w(j)} \tau^{(u)}_{i-w\,\ell} + q'_i \sum_{j=0}^{q-1} \sum_{\ell \in L_{w+1}(j)} \tau^{(u)}_{i-w-1\,\ell} \\
&= d_i^{(u-1)} + \sum_{j=0}^{q-1} \sum_{\ell \in L_w(j)} \left(d_{i-w}^{(u-1)} + \sum_{k=0}^{i-w-1} s_{\ell\,k} d_k^{(u-1)} \right) + q'_i \sum_{j=0}^{q-1} \sum_{\ell \in L_{w+1}(j)} \left(d_{i-w-1}^{(u-1)} + \sum_{k=0}^{i-w-2} s_{\ell\,k} d_k^{(u-1)} \right) \\
&= d_i^{(u-1)} + |E| d_{i-w}^{(u-1)} + \sum_{j=0}^{q-1} \sum_{\ell \in L_w(j)} \sum_{k=0}^{i-w-1} s_{\ell\,k} d_k^{(u-1)} + |F| d_{i-w-1}^{(u-1)} + q'_i \sum_{j=0}^{q-1} \sum_{\ell \in L_{w+1}(j)} \sum_{k=0}^{i-w-2} s_{\ell\,k} d_k^{(u-1)}
\end{aligned}
$$

which concludes the proof of the claim.

Claim 5. $d_i^{(u)} = \sum_{j=0}^{i} \gamma_{i\,j}(u) c_j$, with $\gamma_{i\,j} = \binom{u}{\lfloor \frac{i-j}{w} \rfloor} |E|^{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1})$ for each i which is divisible by w and $\gamma_{i\,j} \leq \binom{u}{\lfloor \frac{i-j}{w} \rfloor} (q \times (q-1))^{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1})$ otherwise.

For $u = 1$ and for each $i = 0, 1, \ldots, \hat{e}$, the claim directly follows by Claim 4, since $|E|, |F| \leq q(q-1)$.

Fix $u > 1$ and $0 \leq i < e$ and assume that the claim is true for each $d_{i'}^{(u')}$ such that either $u' < u$ or $u' = u$ and $i' < i$. We split the analysis into two cases, according to whether or not i is divisible by w.

Case 1. i is divisible by w. By Claim 4 and the induction hypothesis, we have

$$
\begin{aligned}
d_i^{(u)} &= \sum_{j=0}^{i} \delta_{i\,j}^{(u)} d_j^{(u-1)} = d_i^{(u-1)} + |E| d_{i-w}^{(u-1)} + q'_i |F| d_{i-w-1}^{(u-1)} + \sum_{j=0}^{i-w-2} \delta_{i\,j}^{(u-1)} d_j^{(u-1)} \\
&= \sum_{j=0}^{i} c_j \left(\binom{u-1}{\lfloor \frac{i-j}{w} \rfloor} |E|^{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}\left((u-1)^{\lfloor \frac{i-j}{w} \rfloor - 1} \right) \right) \\
&\quad + |E| \sum_{j=0}^{i-w} c_j \left(\binom{u-1}{\lfloor \frac{i-j}{w} \rfloor - 1} |E|^{\lfloor \frac{i-j}{w} \rfloor - 1} + \mathcal{O}\left((u-1)^{\lfloor \frac{i-j}{w} \rfloor - 2} \right) \right) \\
&\quad + q'_i |F| \sum_{j=0}^{i-w-1} c_j \left(\binom{u-1}{\lfloor \frac{i-j-1}{w} \rfloor - 1} (q \times (q-1))^{\lfloor \frac{i-j-1}{w} \rfloor - 1} + \mathcal{O}\left((u-1)^{\lfloor \frac{i-j-1}{w} \rfloor - 2} \right) \right) \\
&\quad + \sum_{j=0}^{i-w-2} c_j \mathcal{O}((u-1)^{\lfloor \frac{i-j-2}{w} \rfloor - 1}) \\
&= \sum_{j=0}^{i} c_j \left(\binom{u-1}{\lfloor \frac{i-j}{w} \rfloor} |E|^{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}((u-1)^{\lfloor \frac{i-j}{w} \rfloor - 1}) \right) \\
&\quad + \sum_{j=0}^{i-w} c_j \left(\binom{u-1}{\lfloor \frac{i-j}{w} \rfloor - 1} |E|^{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}((u-1)^{\lfloor \frac{i-j}{w} \rfloor - 2}) \right) \\
&\quad + \sum_{j=0}^{i-w-1} c_j \mathcal{O}((u-1)^{(\lfloor \frac{i-j-1}{w} \rfloor - 1)})
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{j=i-w+1}^{i} c_j \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} |E|^{\left\lfloor \frac{i-j}{w} \right\rfloor} + \sum_{j=0}^{i-w} c_j |E|^{\left\lfloor \frac{i-j}{w} \right\rfloor} \left(\binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} + \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} \right) \\
&\qquad + \sum_{j=0}^{i} c_j \mathcal{O}((u-1)^{(\left\lfloor \frac{i-j}{w} \right\rfloor - 1)}) \\
&= \sum_{j=i-w+1}^{i} c_j |E|^{\left\lfloor \frac{i-j}{w} \right\rfloor} \binom{u}{\left\lfloor \frac{i-j}{w} \right\rfloor} + \sum_{j=0}^{i-w} c_j |E|^{\left\lfloor \frac{i-j}{w} \right\rfloor} \binom{u}{\left\lfloor \frac{i-j}{w} \right\rfloor} + \sum_{j=0}^{i} c_j \mathcal{O}((u-1)^{\left\lfloor \frac{i-j}{w} \right\rfloor - 1}) \\
&= \sum_{j=0}^{i} c_j \left(|E|^{\left\lfloor \frac{i-j}{w} \right\rfloor} \binom{u}{\left\lfloor \frac{i-j}{w} \right\rfloor} + \mathcal{O}(u^{\left\lfloor \frac{i-j}{w} \right\rfloor - 1}) \right)
\end{aligned}
$$

Case 2. i is not divisible by w. We use again Claim 4 and the induction hypothesis. Moreover we use $|E| + |F| = q(q-1)$ and the fact that, in this case $q'_i = 1$. We have

$$
\begin{aligned}
d_i^{(u)} &= \sum_{j=0}^{i} \delta_{i\,j}^{(u)} d_j^{(u-1)} = d_i^{(u-1)} + |E| d_{i-w}^{(u-1)} + q'_i |F| d_{i-w-1}^{(u-1)} + \sum_{j=0}^{i-w-2} \delta_{i\,j}^{(u-1)} d_j^{(u-1)} \\
&= \sum_{j=0}^{i} c_j \left(\binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} + \mathcal{O}\left((u-1)^{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} \right) \right) \\
&\qquad + |E| \sum_{j=0}^{i-w} c_j \left(\binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} + \mathcal{O}\left((u-1)^{\left\lfloor \frac{i-j}{w} \right\rfloor - 2} \right) \right) \\
&\qquad + q'_i |F| \sum_{j=0}^{i-w-1} c_j \left(\binom{u-1}{\left\lfloor \frac{i-j-1}{w} \right\rfloor - 1} (q \times (q-1))^{\left\lfloor \frac{i-j-1}{w} \right\rfloor - 1} + \mathcal{O}\left((u-1)^{\left\lfloor \frac{i-j-1}{w} \right\rfloor - 2} \right) \right) \\
&\qquad + \sum_{j=0}^{i-w-2} c_j \mathcal{O}((u-1)^{\left\lfloor \frac{i-j-2}{w} \right\rfloor - 1}) \\
&\leq \sum_{j=0}^{i} c_j \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} \\
&\qquad + (q \times (q-1)) \sum_{j=0}^{i-w} c_j \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} \\
&\qquad + \sum_{j=0}^{i} c_j \mathcal{O}((u-1)^{(\left\lfloor \frac{i-j}{w} \right\rfloor - 1)}) \\
&= \sum_{j=i-w+1}^{i} c_j \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} + \sum_{j=0}^{i-w} c_j (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} \left(\binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor - 1} + \binom{u-1}{\left\lfloor \frac{i-j}{w} \right\rfloor} \right) \\
&\qquad + \sum_{j=0}^{i} c_j \mathcal{O}((u-1)^{(\left\lfloor \frac{i-j}{w} \right\rfloor - 1)}) \\
&= \sum_{j=i-w+1}^{i} c_j (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} \binom{u}{\left\lfloor \frac{i-j}{w} \right\rfloor} + \sum_{j=0}^{i-w} c_j (q \times (q-1))^{\left\lfloor \frac{i-j}{w} \right\rfloor} \binom{u}{\left\lfloor \frac{i-j}{w} \right\rfloor}
\end{aligned}
$$

$$+\sum_{j=0}^{i} c_j \mathcal{O}((u-1)^{\lfloor \frac{i-j}{w} \rfloor - 1})$$
$$= \sum_{j=0}^{i} c_j \left((q \times (q-1))^{\lfloor \frac{i-j}{w} \rfloor} \binom{u}{\lfloor \frac{i-j}{w} \rfloor} + \mathcal{O}(u^{\lfloor \frac{i-j}{w} \rfloor - 1}) \right)$$

By Claim 3 we have that both the perfect questions and the states they determine fulfill the integrality constraint.

In order to complete the proof we have to show the existence of an assignment for the c_i's which guarantees that all the questions' and the states' components above are non-negative.

This can be achieved by choosing c_i such that

$$d_i^{(u)} \geq q \left(|E| d_{i-w}^{(u)} + q_i' |F| d_{i-w-1}^{(u)} \right) \qquad \text{for all } u = 0, 1, \ldots . \tag{32}$$

for each $i = 0, 1, \ldots, e$, where $q_i' = q^{\lfloor \frac{i}{w} \rfloor - \lfloor \frac{i-1}{w} \rfloor}$.

In fact, by Claim 3, this gives the desired non-negativity property of the questions, since in equation (31) we have $|L_w(k)| \leq |E|$ and $|L_{w+1}(k)| \leq |F|$ for all k and $\tau_{i-w\,\ell}^{(u)} \leq d_{i-w}^{(u)}$, which imply $\tau_{i\,k}^{(u)} \geq 0$.

Since $d_i^{(u)}, d_{i-w}^{(u)}, d_{i-w-1}^{(u)}$ are polynomials of u and $d_i^{(u)}$ has degree higher than both $d_{i-w}^{(u)}, d_{i-w-1}^{(u)}$, there exists $\lambda = \min_{u \geq 0} d_i^{(u)} - |E| q d_{i-w}^{(u)} - |F| q d_{i-w-1}^{(u)}$. Thus, (32) can be obtained by setting $c_i > -\lambda$. This concludes the proof. □

End of the Proof of Theorem 3

Directly from Proposition 1, Lemma 4 and Theorem 4. □

Acknowledgements

The author would like to thank Joel Spencer for very fruitful comments and remarks on the preliminary version of this paper.

References

[1] L.A. Bassalygo, Nonbinary Error-Correcting Codes with One-Time Error-Free Feedback, Problems of Information Transmission, 41 (2), 125–129, 2005. Translated from Problemy Peredachi Informatsii, 2, 63-67, 2005.

[2] E. R. Berlekamp, Block coding for the binary symmetric channel with noiseless, delayless feedback, in: Error-correcting Codes, H.B. Mann (Editor), Wiley, New York, 61-88, 1968.

[3] F. Cicalese, C. Deppe, and D. Mundici, Q-ary Ulam-Rényi game with weighted constrained lies, Proceedings of the 10th Annual International Conference, COCOON 2004, Jeju Island, Korea, Lecture Notes in Computer Science 3106, Springer–Verlag, 127-132, 2004.

[4] F. Cicalese and C. Deppe, Quasi-perfect minimally adaptive q-ary search with unreliable tests, Proceedings of the 14th International Symposiu, on Algorithms and Computation, ISAAC2003, T. Ibaraki, N. Katoh, H. Ono (Eds.), Lecture Notes in Computer Science 2906, Springer–Verlag, 527-536, 2003.

[5] F. Cicalese and C. Deppe, Q-ary Ulam-Rényi game with constrained lies, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 2006.

[6] F. Cicalese and D. Mundici, Optimal binary search with two unreliable tests and minimum adaptiveness, Proc. European Symposium on Algorithms, ESA '99, J. Nesetril, Ed., Lecture Notes in Computer Science 1643, Springer Verlag, 257-266, 1999.

[7] F. Cicalese, D. Mundici, and U. Vaccaro, Least adaptive optimal search with unreliable tests, Theoretical Computer Science, 270, 877-893, 2002.

[8] F. Cicalese, D. Mundici, and U. Vaccaro, Rota-Metropolis cubic logic and Ulam-Rényi games, Algebraic Combinatorics and Computer Science – A Tribute to Giancarlo Rota, H. Crapo, D. Senato (Eds.), Springer Verlag Italia, Milano, 197-244, 2001.

[9] C. Deppe, Searching with lies and coding with feedback, in *Entropy, Search and Complexity*, G.O.H. Katona (ed.), Bolyai Society Mathematicsl Studies, Vol. **16**, Springer Verlag, Heidelberg, 2006.

[10] I. Dumitriu and J. Spencer, The liar game over an arbitrary channel, Combinatorica 25, 5, 537-559, 2005.

[11] A. Pelc, Searching games with errors – fifty years of coping with liars, Theoret. Comput. Sci., 270, 71–109, 2002.

[12] A. Rényi, On a problem of information theory, MTA Mat. Kut. Int. Kozl., 6B, 505–516, 1961.

[13] S.M. Ulam, Adventures of a Mathematician, Scribner's, New York, 1976.