ELSEVIER

Theoretical Computer Science 270 (2002) 877–893

Theoretical Computer Science

www.elsevier.com/locate/tcs

Mathematical Games

Least adaptive optimal search with unreliable tests ☆

Ferdinando Cicalese[a, *, 1], Daniele Mundici[b, 2], Ugo Vaccaro[a]

[a] *Department of Computer Science and Applications, University of Salerno, Via S. Allende, 84081 Baronissi (SA), Italy*

[b] *Department of Computer Science, University of Milan, Via Comelico 39-41, 20135 Milan, Italy*

Received June 2000; revised January 2001; accepted February 2001
Communicated by A. Fraenkel

Abstract

We consider the basic problem of searching for an unknown m-bit number by asking the minimum possible number of yes–no questions, when up to a finite number e of the answers may be erroneous. In case the $(i+1)$th question is adaptively asked after receiving the answer to the ith question, the problem was posed by Ulam and Rényi and is strictly related to Berlekamp's theory of error correcting communication with noiseless feedback. Conversely, in the fully non-adaptive model when all questions are asked before knowing any answer, the problem amounts to finding a shortest e-error correcting code. Let $q_e(m)$ be the smallest integer q satisfying *Berlekamp's bound* $\sum_{i=0}^{e}\binom{q}{i} \leqslant 2^{q-m}$. Then at least $q_e(m)$ questions are necessary, in the adaptive, as well as in the non-adaptive model. In the fully adaptive case, optimal searching strategies using exactly $q_e(m)$ questions always exist up to finitely many exceptional m's. At the opposite non-adaptive case, searching strategies with exactly $q_e(m)$ questions—or equivalently, e-error correcting codes with 2^m codewords of length $q_e(m)$—are rather the exception, already for $e=2$, and are generally not known to exist for $e>2$. In this paper, for each $e>1$ and all sufficiently large m, we exhibit searching strategies that use a first batch of m non-adaptive questions and then, only depending on the answers to these m questions, a second batch of $q_e(m)-m$ non-adaptive questions. These strategies are automatically optimal. Since even in the fully adaptive case, $q_e(m)-1$ questions do not suffice to find the unknown number, and $q_e(m)$ questions generally do not suffice in the non-adaptive case, the results of our paper provide e fault tolerant searching strategies with minimum adaptiveness and minimum number of tests.

Keywords: Searching; Errors; Lies; Adaptiveness; Codes

☆ A preliminary version of this paper has been presented at SWAT2000, Bergen, Norway, July 2000.

* Corresponding author. Tel.: +39-089-965-416; fax: +39-089-965-272.

E-mail addresses: cicalese@dia.unisa.it (F. Cicalese), mundici@mailserver.unimi.it (D. Mundici), uv@dia.unisa.it (U. Vaccaro).

[1] Supported by ENEA grant.

[2] Partially supported by MURST project on Logic and Applications.

0304-3975/02/$ - see front matter
PII: S0304-3975(01)00116-5

1. Introduction

We consider the following scenario: Two players, called Questioner and Responder, first agree on fixing an integer $m \geqslant 0$ and a search space $S = \{0, \ldots, 2^m - 1\}$. Then the Responder thinks of a number $x_* \in S$ and the Questioner must find out x_* by asking questions to which the Responder can only answer yes or no. It is agreed that the Responder is allowed to lie (or just to be inaccurate) at most e times, where the integer $e \geqslant 0$ is fixed and known to both players.

We are interested in the problem of determining the minimum number of questions the Questioner has to ask in order to infallibly guess the number x_*.

When the questions are asked *adaptively*, i.e., the ith question is asked knowing the answer to the $(i-1)$th question, the problem is generally referred to as the Ulam–Rényi game [37, p. 281; 32, p. 47], and is strictly related to Berlekamp's theory of error correcting communication with noiseless feedback [4] (also see Dobrushin's paper [16]). At the other, *non-adaptive* extreme, when the totality of questions is asked at the outset, before knowing *any* answer, the problem amounts to finding a shortest e error correcting binary code with 2^m codewords.

It is known that at least $q_e(m)$ questions are *necessary* in the adaptive and, a fortiori, in the non-adaptive case—where $q_e(m)$ is the smallest integer q satisfying Berlekamp's bound $\sum_{i=0}^{e} \binom{q}{i} \leqslant 2^{q-m}$.

In the fully adaptive case, an important result of Spencer [34] shows that $q_e(m)$ questions are always sufficient, up to finitely many exceptional m's. Optimal searching strategies had been previously exhibited by Pelc [27], Czyzowicz et al. [14], and Negro and Sereno [26], respectively for the case $e = 1$, 2 and 3. Thus, fully adaptive fault tolerant search can be performed in a very satisfactory manner.

However, in many practical situations it is desirable to have searching strategies with "small degree" of adaptiveness, that is, searching strategies in which all questions (or at least, many of them) can be prepared in advance, and asked in parallel. This is the case, e.g., when the Questioner and the Responder are far away from each other and can interact only on a slow channel; or, in all situations when the mere formulation of each query is a costly process, and therefore the Questioner finds it more convenient and time saving to prepare all questions in advance. We refer to the monographs [1, 17] for a discussion on the power of adaptive and non-adaptive searching strategies and their possible uses in different contexts.

Unfortunately, in the totally non-adaptive case, searching strategies with exactly $q_e(m)$ questions—or equivalently, binary e error correcting codes with 2^m codewords of length $q_e(m)$—are sporadic exceptions already for $e = 2$, and are generally not known to exist for $e > 2$, except in trivial cases. Moreover, a series of negative results culminating in the celebrated papers by Tietäväinen [36] and Zinoviev–Leontiev [39] (also see [22]) shows that if $q = q_e(m)$, is such that $\sum_{i=0}^{e} \binom{q}{i} = 2^{q-m}$, then e error correcting codes of length q with 2^m codewords *do not exist* for all $e > 2$.[3] Thus, in general,

[3] The only exceptions are the Golay code ($m = 12, e = 3$) [18] and the trivial repetition codes ($m = 1, e \geqslant 1$); the latter codes only contain two words, $\{111\cdots1, 000\cdots0\}$, each of length $2e+1$.

adaptiveness in Ulam–Rényi games can be completely eliminated *only by significantly increasing the number of questions in the solution strategy*.[4]

Our purpose in this paper is to investigate the minimum amount of adaptiveness required by any successful searching strategy with exactly $q_e(m)$ questions.

1.1. Our results

We exactly quantify the minimum amount of adaptiveness needed to solve the Ulam–Rényi problem, while still constraining the total number of questions to Berlekamp's minimum $q_e(m)$. Our main result is that for each e, and for all sufficiently large m, there exist searching strategies of shortest length (using *exactly* the minimum number $q_e(m)$ of questions) in which questions can be submitted to the Responder in *only two* rounds. Specifically, for the Questioner to infallibly guess the Responder's secret number $x_* \in S$ it is *sufficient* to ask a first batch of m non-adaptive questions, and then, only depending on the m-tuple of answers, ask a second mini-batch of n non-adaptive questions. Our strategies are *perfect*, in that $m+n$ coincides with Berlekamp's minimum $q_e(m)$, the number of questions that are a priori *necessary* to accommodate all possible answering strategies of the Responder—once he is allowed to lie up to e times. Since the Questioner can adapt his strategy only once, our paper yields e fault tolerant search strategies with *minimum* adaptiveness and the least possible number of tests. As we shall see in Section 3, our results mainly rely on the correspondence between e fault tolerant searching strategies, and certain non-uniform error correcting codes. In Section 5, focusing on the case $e=3$, we shall give an explicit description of our searching strategies for the Ulam–Rényi game, for all $m \geqslant 99$. Finally, in Section 6 we shall be concerned with the problem of *shrinking the first batch of questions*: this is equivalent to the concrete problem of minimizing the number of bits to be sent over the expensive noiseless feedback channel of Berlekamp's theory [4].

1.2. Related work

The general issue of coping with unreliable information (and/or unreliable components) in computing is an important problem in computer science, its study going back to the work of von Neumann [38]. After the pioneering paper [33], the problem of dealing with erroneous information in search strategies (what we call here the Ulam–Rényi game) has received rapidly increasing attention in the last two decades (see, e.g., [3, 2, 5, 13–15, 25, 27, 34] and references therein). Also see the survey papers [12, 19, 30].

Besides its relationship with Berlekamp's theory of error correcting communication with noiseless feedback [4], the Ulam–Rényi game has several interesting connections with various areas of computer science, combinatorics and logic (see for instance [7, 23, 20, 12]). It is not our aim in this paper to cover these topics: we shall only limit

[4] The situation is completely different in the case of no lies: here an optimal, totally non-adaptive searching strategy with $\lceil \log |S| \rceil$ questions simply amounts to asking $\lceil \log |S| \rceil$ queries about the locations of the bit 1 in the binary expansion of the unknown number $x_* \in S$.

ourselves to mentioning those results which are directly related to our present issue of adaptive vs. non-adaptive search.

Skipping the trivial case $e=0$, for $e=1$ Hamming codes turn out to yield non-adaptive (also called, *one round*) searching strategies with the smallest possible number $q_1(m)$ of questions. Further, Pelc [29] showed that adaptiveness is irrelevant even under the stronger assumption that repetition of the same question is forbidden.

The first significant occurrence of the dichotomy between adaptive and non-adaptive search is for $e=2$. Two-round optimal strategies for the case $e=2$ were given in [9]. Our paper extends the result of [9] to the case of an *arbitrary* number e of errors/lies. See [15, 35] for more results about adaptive vs. non-adaptive searching strategies.

2. The Ulam–Rényi game

For some fixed integer $m \geqslant 0$, let $S=\{0,1,\ldots,2^m-1\}$ be the search space. By a *yes–no question* we simply mean an arbitrary subset T of S. If the answer to the question T is "yes", numbers in T are said to *satisfy* the answer, while numbers in $S\backslash T$ *falsify* it. A negative answer to question T has the same effect as a positive answer to the opposite question $S\backslash T$. At any stage of the game, a number $y\in S$ must be rejected from consideration if, and only if, it falsifies more than e answers. The remaining numbers of S still are possible candidates for the unknown x_*.

At any time during the game, the Questioner's *state* of knowledge is represented by an e-tuple $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ of pairwise disjoint subsets of S, where A_i is the set of numbers falsifying exactly i answers, $i=0,1,2,\ldots,e$. The *initial* state is naturally given by $(S,\emptyset,\emptyset,\ldots,\emptyset)$. A state $(A_0,A_1,A_2\ldots,A_e)$ is *final* iff $A_0\cup A_1\cup A_2\cup\cdots\cup A_e$ either has exactly one element, or is empty.

For any state $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ and question $T\subseteq S$, the two states σ^{yes} and σ^{no}, respectively resulting from a positive or a negative answer, are given by

$$\sigma^{\text{yes}}=(A_0^{\text{yes}},A_1^{\text{yes}},\ldots,A_e^{\text{yes}}) \quad \text{and} \quad \sigma^{\text{no}}=(A_0^{\text{no}},A_1^{\text{no}},\ldots,A_e^{\text{no}}), \tag{1}$$

where, for the sake of definiteness, we let $A_{-1}=\emptyset$, and

$$A_i^{\text{yes}}=(A_i\cap T)\cup(A_{i-1}\backslash T) \quad \text{and} \quad A_i^{\text{no}}=(A_i\backslash T)\cup(A_{i-1}\cap T) \tag{2}$$

for each $i=0,1,\ldots,e$. Given a state σ, suppose questions $T_1,\ldots,T_t$ have been asked and answers $\boldsymbol{b}=b_1,\ldots,b_t$ have been received (with $b_i\in\{\text{yes},\text{no}\}$). Iterated application of the above formulas yields a sequence of states

$$\sigma_0=\sigma, \quad \sigma_1=\sigma_0^{b_1}, \quad \sigma_2=\sigma_1^{b_2},\ldots,\sigma_t=\sigma_{t-1}^{b_t}. \tag{3}$$

By a *strategy* $\mathscr{S}$ with q questions we mean the binary tree of depth q, where each node v is mapped into a question T_v, and the two edges $\eta_{\text{left}},\eta_{\text{right}}$ generated by v are, respectively, labelled *yes* and *no*. Let $\boldsymbol{\eta}=\eta_1,\ldots,\eta_q$ be a path in $\mathscr{S}$, from the root to a leaf, with respective labels $b_1,\ldots,b_q$, generating nodes $v_1,\ldots,v_q$ and

associated questions $T_{v_1},\ldots,T_{v_q}$. Fix an arbitrary state σ. Then, according to (3), iterated application of (1) and (2) naturally transforms σ into $\sigma^{\boldsymbol{\eta}}$ (where the dependence on the b_j and T_j is understood). We say that strategy $\mathscr{S}$ is *winning* for σ iff for every path $\boldsymbol{\eta}$ the state $\sigma^{\boldsymbol{\eta}}$ is final. A strategy is said to be *non-adaptive* iff all nodes at the same depth of the tree are mapped into the same question.

Let $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ be a state. For each $i=0,1,2,\ldots,e$ let $a_i=|A_i|$ be the number of elements of A_i. Then the e-tuple $(a_0,a_1,a_2,\ldots,a_e)$ is called the *type* of σ. The *Berlekamp weight of σ before q questions*, $q=0,1,2,\ldots$, is given by

$$w_q(\sigma)=\sum_{i=0}^{e}a_i\sum_{j=0}^{e-i}\binom{q}{j}. \tag{4}$$

The *character* $\mathrm{ch}(\sigma)$ of a state σ is the smallest integer $q\geqslant 0$ such that $w_q(\sigma)\leqslant 2^q$.

By abuse of notation, the weight of *any* state σ of type $(a_0,a_1,a_2,\ldots,a_e)$ before q questions will be denoted $w_q(a_0,a_1,a_2,\ldots,a_e)$. Similarly, its character will also be denoted $\mathrm{ch}(a_0,a_1,a_2,\ldots,a_e)$.

As an immediate consequence of the above definition we have the following monotonicity properties: For any two states $\sigma'=(A'_0,A'_1,A'_2,\ldots,A'_e)$ and $\sigma''=(A''_0,A''_1,A''_2,\ldots,A''_e)$ respectively of type $(a'_0,a'_1,a'_2,\ldots,a'_e)$ and $(a''_0,a''_1,a''_2,\ldots,a''_e)$, if $a'_i\leqslant a''_i$ for all $i=0,1,2,\ldots,e$ then

$$\mathrm{ch}(\sigma')\leqslant\mathrm{ch}(\sigma'')\quad\text{and}\quad w_q(\sigma')\leqslant w_q(\sigma'') \tag{5}$$

for each $q\geqslant 0$. Moreover, if there exists a winning strategy for σ'' with q questions then there exists also a winning strategy for σ' with q questions [4]. Note that $\mathrm{ch}(\sigma)=0$ iff σ is a final state.

Lemma 2.1 (Berlekamp [4]). *Let σ be an arbitrary state, and $T\subseteq S$ a question. Let σ^{yes} and σ^{no} be as in* (1) *and* (2).

(i) (Conservation Law). *For any integer $q\geqslant 1$ we have $w_q(\sigma)=w_{q-1}(\sigma^{\mathrm{yes}})+w_{q-1}(\sigma^{\mathrm{no}})$.*

(ii) (Berlekamp's lower bound). *If σ has a winning strategy with q questions then $q\geqslant\mathrm{ch}(\sigma)$.*

A strategy $\mathscr{S}$ of size q for a state σ is said to be *perfect* if $\mathscr{S}$ is winning for σ and $q=\mathrm{ch}(\sigma)$.[5] In agreement with the above notation, we shall write $q_e(m)$ instead of $\mathrm{ch}(2^m,0,\ldots,0)$.

Let $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ be a state. Let $T\subseteq S$ be a question. We say that T is *balanced for* σ iff for each $j=0,1,2,\ldots,e$, we have $|A_j\cap T|=|A_j\backslash T|$.

The following is easy to prove.

Lemma 2.2. *Let T be a balanced question for a state $\sigma=(A_0,A_1,A_2,\ldots,A_e)$. Let $n=\mathrm{ch}(\sigma)$. Let σ^{yes} and σ^{no} be as in* (1) *and* (2) *above. Then*

[5] There shall be no danger of confusion between the usual meaning of "perfect code", and the present generalization. Because a perfect strategy $\mathscr{S}$ uses the least possible number of questions, as given by Berlekamp's bound, $\mathscr{S}$ is *optimal*, in the sense that it cannot be superseded by a shorter strategy.

(i) $w_q(\sigma^{\text{yes}}) = w_q(\sigma^{\text{no}})$, *for each integer* $q \geqslant 0$,
(ii) $\text{ch}(\sigma^{\text{yes}}) = \text{ch}(\sigma^{\text{no}}) = n - 1$.

3. Strategies vs. codes

We refer to [22] for background in error correcting codes. Here we shall only fix a few notions and notations for later use.

Fix an integer $n > 0$ and let $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$. The *Hamming distance* $d_H(\boldsymbol{x}, \boldsymbol{y})$ is defined by

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|,$$

where, as above, $|A|$ denotes the number of elements of A, and x_i (resp. y_i) denotes the ith components of $\boldsymbol{x}$ (resp. $\boldsymbol{y}$).

The *Hamming sphere* $\mathscr{B}_r(\boldsymbol{x})$ *with radius* r *and center* $\boldsymbol{x}$ is the set of elements of $\{0,1\}^n$ whose Hamming distance from $\boldsymbol{x}$ is at most r, in symbols,

$$\mathscr{B}_r(\boldsymbol{x}) = \{\boldsymbol{y} \in \{0,1\}^n \mid d_H(\boldsymbol{x}, \boldsymbol{y}) \leqslant r\}.$$

Notice that for any $\boldsymbol{x} \in \{0,1\}^n$, and $r \geqslant 0$, we have $|\mathscr{B}_r(\boldsymbol{x})| = \sum_{i=0}^{r} \binom{n}{i}$. The *Hamming weight* $w_H(\boldsymbol{x})$ of $\boldsymbol{x}$ is the number of non-zero digits of $\boldsymbol{x}$. Throughout this paper, by a code we shall mean a binary code, in the following sense:

Definition 3.1. A (*binary*) *code* $\mathscr{C}$ *of length* n is a non-empty subset of $\{0,1\}^n$. Its elements are called *codewords*. The *minimum distance* of $\mathscr{C}$ is given by

$$\delta(\mathscr{C}) = \min\{d_H(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in \mathscr{C}, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

We say that $\mathscr{C}$ is an (n, M, d) *code* iff $\mathscr{C}$ has length n, $|\mathscr{C}| = M$ and $\delta(\mathscr{C}) = d$. The *minimum weight* of $\mathscr{C}$ is the minimum of the Hamming weights of its codewords, in symbols,

$$\mu(\mathscr{C}) = \min\{w_H(\boldsymbol{x}) \mid \boldsymbol{x} \in \mathscr{C}\}.$$

Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be two codes of length n. The *minimum distance between* $\mathscr{C}_1$ *and* $\mathscr{C}_2$ is defined by

$$\Delta(\mathscr{C}_1, \mathscr{C}_2) = \min\{d_H(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x} \in \mathscr{C}_1, \boldsymbol{y} \in \mathscr{C}_2\}.$$

The following lemma is known as Gilbert's bound [22].

Lemma 3.2. *Let* $n = 2, 3, \ldots$. *Then for any two integers* $1 \leqslant d \leqslant n$, *and*

$$1 \leqslant M \leqslant \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}},$$

there exists an (n, M, d) *binary code* $\mathscr{C}$.

We now describe a correspondence between non-adaptive winning strategies and certain special codes. This will be a key tool to prove the main results of our paper.

Lemma 3.3. *Fix an integer* $e=1,2,3,\ldots$. *Let* $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ *be a state of type* $(a_0,a_1,a_2,\ldots,a_e)$. *Let* $n \geqslant \mathrm{ch}(\sigma)$. *Then a non-adaptive winning strategy for* σ *with* n *questions exists* if and only if *for all* $i=0,1,2,\ldots,e-1$ *there are integers* $d_i \geqslant 2(e-i)+1$, *together with an* e*-tuple of codes* $\Gamma=(\mathscr{C}_0,\mathscr{C}_1,\mathscr{C}_2,\ldots,\mathscr{C}_{e-1})$, *such that each* $\mathscr{C}_i$ *is an* (n,a_i,d_i) *code, and* $\Delta(\mathscr{C}_i,\mathscr{C}_j) \geqslant 2e-(i+j)+1$, *(whenever* $0 \leqslant i<j \leqslant e-1$).

Proof. We first prove the implication *strategy* $\Rightarrow$ *codes*.

Assume $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ to be a state of type $(a_0,a_1,a_2,\ldots,a_e)$ having a non-adaptive winning strategy $\mathscr{S}$ with n questions $T_1,\ldots,T_n$, $n \geqslant \mathrm{ch}(\sigma)$. Let the map

$$z \in A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_e \mapsto \boldsymbol{z}^{\mathscr{S}} \in \{0,1\}^n$$

send each $z \in A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_e$ into the n-tuple of bits $\boldsymbol{z}^{\mathscr{S}}=z_1^{\mathscr{S}}\cdots z_n^{\mathscr{S}}$ arising from the sequence of "true" answers to the questions "does z belong to T_1?", "does z belong to T_2?" ,..., "does z belong to T_n?", via the identifications $1=yes$, $0=no$. More precisely, for each $j=1,\ldots,n$, $z_j^{\mathscr{S}}=1$ iff $z \in T_j$. Let $\mathscr{C} \subseteq \{0,1\}^n$ be the range of the map $z \mapsto \boldsymbol{z}^{\mathscr{S}}$. We shall first prove that, for every $i=0,\ldots,e-1$, there exists an integer $d_i \geqslant 2(e-i)+1$ such that the set $\mathscr{C}_i=\{\boldsymbol{y}^{\mathscr{S}} \in \mathscr{C} \mid y \in A_i\}$ is an (n,a_i,d_i) code.

Since $\mathscr{S}$ is winning, the map $z \mapsto \boldsymbol{z}^{\mathscr{S}}$ is one to one, whence in particular $|\mathscr{C}_i|=a_i$, for any $i=0,1,2,\ldots,e-1$. Moreover by definition, the $\mathscr{C}_i$'s are subsets of $\{0,1\}^n$.

Claim 1. $\delta(\mathscr{C}_i) \geqslant 2(e-i)+1$, *for* $i=0,\ldots,e-1$.

For otherwise (absurdum hypothesis) assuming c and d to be two distinct elements of A_i such that $d_H(\boldsymbol{c}^{\mathscr{S}},\boldsymbol{d}^{\mathscr{S}}) \leqslant 2(e-i)$, we will prove that $\mathscr{S}$ is not a winning strategy. We can safely assume $c_j^{\mathscr{S}}=d_j^{\mathscr{S}}$ for each $j=1,\ldots,n-2(e-i)$. Suppose the answer to question T_j is "yes" or "no" according as $c_j^{\mathscr{S}}=1$ or $c_j^{\mathscr{S}}=0$, respectively. Then after $n-2(e-i)$ answers, the resulting state has the form $\sigma'=(A_0',\ldots,A_i',\ldots,A_e')$, with $\{c,d\} \subseteq A_i'$, whence the type of σ' is $(a_0',\ldots,a_i',\ldots,a_e')$ with $a_i' \geqslant 2$. Since by Berlekamp [4, Lemma 2.5], $\mathrm{ch}(\sigma') \geqslant \mathrm{ch}(0,0,\ldots,0,2,0,\ldots,0)=2(e-i)+1$ then from Lemma 2.1(ii) it follows that the remaining $2(e-i)$ questions/answers do not suffice to reach a final state, thus contradicting the assumption that $\mathscr{S}$ is winning.

Claim 2. *For any* $0 \leqslant i<j \leqslant e-1$ *and for each* $y \in A_i$ *and* $h \in A_j$ *we have the inequality* $d_H(\boldsymbol{y}^{\mathscr{S}},\boldsymbol{h}^{\mathscr{S}}) \geqslant 2e-(i+j)+1$.

For otherwise (absurdum hypothesis) let $y \in A_i, h \in A_j$ be a counterexample, and $d_H(\boldsymbol{y}^{\mathscr{S}},\boldsymbol{h}^{\mathscr{S}}) \leqslant 2e-(i+j)$. Writing $\boldsymbol{y}^{\mathscr{S}}=y_1^{\mathscr{S}}\ldots y_n^{\mathscr{S}}$ and $\boldsymbol{h}^{\mathscr{S}}=h_1^{\mathscr{S}}\ldots h_n^{\mathscr{S}}$, it is no loss of generality to assume $h_k^{\mathscr{S}}=y_k^{\mathscr{S}}$, for all $k=1,\ldots,n-(2e-(i+j))$. Suppose that the answer to question T_k is "yes" or "no" according as $h_k^{\mathscr{S}}=1$ or $h_k^{\mathscr{S}}=0$, respectively. Then the state resulting from these answers has the form $\sigma''=(A_0'',A_1'',A_2'',\ldots,A_e'')$, where $y \in A_i''$ and $h \in A_j''$. Since by Berlekamp [4, Lemma 2.5], $\mathrm{ch}(\sigma'') \geqslant \mathrm{ch}(0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)=2e-(i+j)+1$, then Lemma 2.1(ii) again shows that $2e-(i+j)$ additional

questions will not suffice to find the unknown number. This contradicts the assumption that $\mathscr{S}$ is a winning strategy.

In conclusion, for all $i=0,1,\ldots,e-1$, $\mathscr{C}_i$ is an (n,a_i,d_i) code with $d_i \geqslant 2(e-i)+1$ and for all $j=0,\ldots,i-1,i+1,\ldots,e-1$, we have the desired inequality $\Delta(\mathscr{C}_i,\mathscr{C}_j) \geqslant 2e-(i+j)+1$.

Now we prove the converse implication: *strategy* $\Leftarrow$ *codes*.

Let $\Gamma=(\mathscr{C}_0,\mathscr{C}_1,\mathscr{C}_2,\ldots,\mathscr{C}_{e-1})$ be an e-tuple of codes satisfying the hypothesis. Let

$$\mathscr{H}=\bigcup_{i=0}^{e-1}\bigcup_{\boldsymbol{x}\in\mathscr{C}_i}\mathscr{B}_{e-i}(\boldsymbol{x}).$$

By hypothesis, for any $i,j\in\{0,1,\ldots,e-1\}$ and $\boldsymbol{x}\in\mathscr{C}_i$, $\boldsymbol{y}\in\mathscr{C}_j$ we have $d_H(\boldsymbol{x},\boldsymbol{y}) \geqslant 2e-(i+j)+1$. It follows that the Hamming spheres $\mathscr{B}_{e-i}(\boldsymbol{x}),\mathscr{B}_{e-j}(\boldsymbol{y})$ are pairwise disjoint and hence

$$|\mathscr{H}|=\sum_{i=0}^{e-1}a_i\sum_{j=0}^{e-i}\binom{n}{j}. \tag{6}$$

Let $\mathscr{D}=\{0,1\}^n\backslash\mathscr{H}$. Since $n \geqslant \mathrm{ch}(a_0,a_1,a_2,\ldots,a_e)$, by definition of character we have $2^n \geqslant \sum_{i=0}^{e}a_i\sum_{j=0}^{e-i}\binom{n}{j}$. From (6) it follows that

$$|\mathscr{D}|=2^n-\sum_{i=0}^{e-1}a_i\sum_{j=0}^{e-i}\binom{n}{j} \geqslant a_e. \tag{7}$$

Let $\sigma=(A_0,A_1,A_2,\ldots,A_e)$ be an arbitrary state of type $(a_0,a_1,a_2,\ldots,a_e)$. Let us now fix, once and for all, $e+1$ one–one maps $f_i:A_i\to\mathscr{C}_i$, for $i=0,1,\ldots,e-1$ and $f_e:A_e\to\mathscr{D}$. The existence of the map f_i, for all $i=0,1,\ldots,e$, is ensured by our assumptions about Γ, together with (7).

Let the map $f:A_0\cup A_1\cup A_2\cup\cdots\cup A_e\to\{0,1\}^n$ be defined by cases as follows:

$$f(y)=\begin{cases} f_0(y),\ y\in A_0\\ f_1(y),\ y\in A_1\\ \vdots\\ f_e(y),\ y\in A_e.\end{cases} \tag{8}$$

Note that f is one–one. For each $y\in A_0\cup A_1\cup A_2\cup\cdots\cup A_e$ and $j=1,\ldots,n$ let $f(y)_j$ be the jth bit of the n-tuple $f(y)\in\{0,1\}^n$. We can now exhibit the questions T_j of our searching strategies:

For each $j=1,\ldots,n$ let the set $T_j\subseteq S$ be defined by $T_j=\{z\in\bigcup_{i=0}^{e}A_i \mid f(z)_j=1\}$.

Intuitively, letting x_* denote the unknown number, T_j asks "is the jth bit of $f(x_*)$ equal to one ?"

Again writing yes $=1$ and no $=0$, the answers to questions $T_1,\ldots,T_n$ determine an n-tuple of bits $\boldsymbol{b}=b_1\cdots b_n$. We shall show that the sequence $T_1,\ldots,T_n$ yields an optimal

non-adaptive winning strategy for σ. Let $\sigma_1=\sigma^{b_1}, \sigma_2=\sigma_1^{b_2}, \ldots, \sigma_n=\sigma_{n-1}^{b_n}$. Arguing by cases we shall show that $\sigma_n=(A_0^*, A_1^*, \ldots, A_e^*)$ is a final state.

By (1) and (2), for all $i=0,1,\ldots,e$, any $z\in A_{e-i}$ that falsifies $>i$ answers does not survive in σ_n—in the sense that $z\notin A_0^*\cup A_1^*\cup\cdots\cup A_e^*$.

Case 1: $\boldsymbol{b}\notin\bigcup_{i=0}^{e}\bigcup_{y\in A_i}\mathscr{B}_{e-i}(f(y))$. For all $i=0,1,\ldots,e$, and for each $y\in A_i$ we must have $y\notin A_0^*\cup A_1^*\cup\cdots\cup A_e^*$. Indeed, the assumption $\boldsymbol{b}\notin\mathscr{B}_{e-i}(f(y))$ implies $d_H(f(y),\boldsymbol{b})>e-i$, whence y falsifies $>e-i$ of the answers to $T_1,\ldots,T_n$, and y does not survive in σ_n. We have proved that $A_0^*\cup A_1^*\cup\cdots\cup A_e^*$ is empty, and σ_n is a final state.

Case 2: $\boldsymbol{b}\in\mathscr{B}_{e-i}(f(y))$ for some $i\in\{0,1,\ldots,e\}$ and $y\in A_i$. Then $y\in A_0^*\cup A_1^*\cup\cdots\cup A_e^*$, because $d_H(f(y),\boldsymbol{b})\leqslant e-i$, whence y falsifies $\leqslant e-i$ answers. Our assumptions about Γ ensure that, for all $j=0,1,\ldots,e$ and for all $y'\in A_j$ and $y\neq y'$, we have $\boldsymbol{b}\notin\mathscr{B}_{e-j}(f(y'))$. Thus, $d_H(f(y'),\boldsymbol{b})>e-j$ and y' falsifies $>e-j$ of the answers to $T_1,\ldots,T_n$, whence y' does not survive in σ_n. This shows that for any $y'\neq y$, we have $y'\notin A_0^*\cup A_1^*\cup\cdots\cup A_e^*$. Therefore, $A_0^*\cup A_1^*\cup\cdots\cup A_e^*$ only contains the element y, and σ_n is a final state. □

4. Optimal strategies with minimum adaptiveness

4.1. The first batch of questions

As the reader will recall, for any two integers $e,m\geqslant 0$ we denote by $q_e(m)=\mathrm{ch}(2^m, 0,\ldots,0)$ the smallest integer $q\geqslant 0$ such that $2^q\geqslant 2^m(\binom{q}{e}+\binom{q}{e-1}+\cdots+\binom{q}{2}+q+1)$. By Lemma 2.1(ii), at least $q_e(m)$ questions are *necessary* to guess the unknown number $x_*\in S=\{0,1,\ldots,2^m-1\}$, if up to e answers may be erroneous. The aim of the rest of this paper is to prove that, conversely, for all suitably large m, $q_e(m)$ questions are *sufficient* under the following constraint: first we use a predetermined non-adaptive batch of m questions $D_1,\ldots,D_m$, and then, only depending on the answers, we ask the remaining $q_e(m)-m$ questions in a second non-adaptive batch.

The *first batch of questions* is easily described as follows:

> For each $i=1,2,\ldots,m$, let $D_i\subseteq S$ denote the question "Is the ith binary digit of x_* equal to 1?" Thus a number $y\in S$ belongs to D_i iff the ith bit y_i of its binary expansion $\boldsymbol{y}=y_1\cdots y_m$ is equal to 1.

Upon identifying $1=$yes and $0=$no, let $b_i\in\{0,1\}$ be the answer to question D_i. Let $\boldsymbol{b}=b_1\cdots b_m$. Repeated applications of (1) and (2) beginning with the initial state $\sigma=(S,\emptyset,\ldots,\emptyset)$, shows that the resulting state as an effect of the answers $b_1\cdots b_m$, is an $(e+1)$-tuple $\sigma^{\boldsymbol{b}}=(A_0,A_1,\ldots,A_e)$, where

$$A_i=\{y\in S\mid d_H(\boldsymbol{y},\boldsymbol{b})=i\}\quad\text{for all } i=0,1,\ldots,e.$$

Direct verification yields

$$|A_0|=1,\quad |A_1|=m,\ldots,|A_e|=\binom{m}{e}.$$

Thus $\sigma^{\boldsymbol{b}}$ has type $(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$. As in (3), let σ_i be the state resulting after the first i answers, beginning with $\sigma_0 = \sigma$. Since each question D_i is balanced for σ_{i-1}, an easy induction using Lemma 2.2 yields $\mathrm{ch}(\sigma^{\boldsymbol{b}}) = q_e(m) - m$.

For each m-tuple $\boldsymbol{b} \in \{0,1\}^m$ of possible answers, we shall construct a non-adaptive strategy $\mathscr{S}_{\boldsymbol{b}}$ with $\mathrm{ch}(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$ questions, which turns out to be winning for the state $\sigma^{\boldsymbol{b}}$. To this purpose, let us consider the values of $\mathrm{ch}(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$ for $m \geqslant 1$.

Definition 4.1. Let $e \geqslant 0$ and $n \geqslant 2e$ be arbitrary integers. The *critical index* $m_{n,e}$ is the largest integer $m \geqslant 0$ such that $\mathrm{ch}(1, m, \binom{m}{2}, \ldots, \binom{m}{e}) = n$.

Lemma 4.2. *Let $e \geqslant 1$ and $n \geqslant 2e$ be arbitrary integers. Then $m_{n,e} < \sqrt[e]{e!}\, 2^{n/e} + e$.*

Proof. By definition, $m_{n,e} = \max\{m \mid w_n(1, m, \binom{m}{2}, \ldots, \binom{m}{e}) \leqslant 2^n\}$. Setting now $m^* = \sqrt[e]{e!}\, 2^{n/e} + e$, the desired result directly follows from the inequality $w_n(1, m^*, \binom{m^*}{2}, \ldots, \binom{m^*}{e}) > 2^n$. As a matter of fact,

$$w_n\left(1, m^*, \binom{m^*}{2}, \ldots, \binom{m^*}{e}\right) > w_n\left(0, 0, \ldots, 0, \binom{m^*}{e}\right)$$

$$= \binom{m^*}{e} = \frac{m^*(m^*-1)\cdots(m^*-e+1)}{e!}$$

$$\geqslant \frac{(\sqrt[e]{e!}\, 2^{n/e})^e}{e!} = 2^n. \qquad \square$$

4.2. The second batch of questions

We now prove that for all sufficiently large m there exists a second batch of $n = q_e(m) - m = \mathrm{ch}(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$ non-adaptive questions allowing the Questioner to infallibly guess the Responder's secret number. We first need the following lemma. [6]

Lemma 4.3. *For any fixed $e = 1, 2, \ldots$ and all sufficiently large integers n, there exists an e-tuple of codes $\Gamma = (\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_{e-1})$ together with integers $d_i \geqslant 2(e-i) + 1$ $(i = 0, 1, \ldots, e-1)$ such that*

(i) *Each $\mathscr{C}_i$ is an $(n, \binom{m_{n,e}}{i}, d_i)$ code;*

(ii) $\Delta(\mathscr{C}_i, \mathscr{C}_j) \geqslant 2e - (i+j) + 1$, *(whenever $0 \leqslant i < j \leqslant e-1$).*

Proof. Let $n' = n - e^2$. First we prove the existence of an $(n', \binom{m_{n,e}}{e-1}, d')$ code, with $d' = 2e + 1$. From Lemma 4.2 together with the trivial inequality $e! \leqslant (e+1)^e/2^e$, it

[6] The problem of finding families of error-correcting codes with fixed reciprocal distances was also addressed in [40], where the authors proved a result related to our Lemma 4.3 showing the existence of asymptotically optimal such families.

follows that, for all sufficiently large n

$$\begin{aligned}\binom{m_{n,e}}{e-1} &< (m_{n,e})^{e-1}\\ &< (\sqrt[e]{e!}\,2^{n/e}+e)^{e-1}\\ &\leqslant (e2^{n/e})^{e-1}\\ &= e^{e-1}2^{n-n/e}\\ &= e^{e-1}\frac{2^{n-e^2}}{2^{n/e-e^2}}\\ &\leqslant \frac{2^{n-e^2}}{\sum_{j=0}^{2e}\binom{n-e^2}{j}},\end{aligned}$$

since $\sum_{j=0}^{2e}\binom{n-e^2}{j}$ is polynomial in n.

The existence of the desired $(n',\binom{m_{n,e}}{e-1},d')$ code now follows from Gilbert's Bound. We have proved that, for all sufficiently large n, there exists an $(n-e^2,\binom{m_{n,e}}{e-1},d')$ code $\mathscr{C}'$ with $d'\geqslant 2e+1$. For each $i=0,1,\ldots,e-1$ let the e^2-tuple $\boldsymbol{a}_i$ be defined by

$$\boldsymbol{a}_i=\underbrace{00\ldots0}_{ie}\ \underbrace{11\ldots1}_{e}\ \underbrace{0\ldots0}_{e^2-(i+1)e}.$$

Furthermore, let $\mathscr{C}_i''$ be the code obtained by appending the suffix $\boldsymbol{a}_i$ to the codewords of $\mathscr{C}'$, in symbols,

$$\mathscr{C}_i''=\mathscr{C}'\otimes\boldsymbol{a}_i.$$

Trivially, $\mathscr{C}_i''$ is an $(n,\binom{m_{n,e}}{e-1},2e+1)$ code for all $i=0,1,\ldots,e-1$. Furthermore, we have $\Delta(\mathscr{C}_i'',\mathscr{C}_j'')=2e\geqslant 2e-(i+j)+1$, whenever $0\leqslant i<j\leqslant e-1$. For each $i=0,1,\ldots,e-1$, pick a subcode $\mathscr{C}_i\subseteq\mathscr{C}_i''$ with $|\mathscr{C}_i|=\binom{m_{n,e}}{i}$. Then the new e-tuple of codes $\Gamma=(\mathscr{C}_0,\mathscr{C}_1,\ldots,\mathscr{C}_{e-1})$ satisfies both conditions (i) and (ii), and the proof is complete. □

The following corollary implies the existence of minimum adaptiveness perfect searching strategies.

Corollary 4.4. *Fix an integer $e\geqslant 0$. Then for all sufficiently large integers m and for every state σ of type $(1,m,\binom{m}{2},\ldots,\binom{m}{e})$ there exists a non-adaptive winning strategy $\mathscr{S}$ such that the number of questions in $\mathscr{S}$ coincides with Berlekamp's lower bound* $\mathrm{ch}(\sigma)=q_e(m)-m$.

Proof. Skipping all trivialities, assume $e\geqslant 1$. Let $n=\mathrm{ch}(\sigma)$. By definition, $n\to\infty$ as $m\to\infty$. Lemmas 4.3 and 3.3 yield a non-adaptive winning strategy with n questions for any state of type $(1,m_{n,e},\binom{m_{n,e}}{2},\ldots,\binom{m_{n,e}}{e})$. By Definition 4.1, $m\leqslant m_{n,e}$, and a

fortiori, for all sufficiently large m, a non-adaptive winning strategy with n questions exists for any state of type $(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$. □

5. Ulam–Rényi game with three lies and minimum adaptiveness

In this section we restrict to the particular case $e = 3$. We recall that two-round optimal strategies for the case $e = 2$ were given in [9]. We shall prove that for all $m \geqslant 99$ *perfect* (hence, a fortiori, optimal) searching strategies do exist to find an unknown m-bit number x_* with minimum adaptiveness and up to three lies in the answers. States now have the form (A_0, A_1, A_2, A_3). Proceeding as in the previous section, we may safely assume that after a first batch of m non-adaptive questions asking for the binary expansion of x_*, the resulting state σ is of type $(1, m, \binom{m}{2}, \binom{m}{3})$ and character $n = \mathrm{ch}(\sigma) = q_3(m) - m$. We shall explicitly describe non-adaptive winning strategies with n questions for such σ, whenever $m \geqslant 99$.[7] We shall use the following preliminary lemma.

Lemma 5.1. *Let n and m be arbitrary integers $\geqslant 1$. For each $i = 1, 2$, let $\mathscr{C}_i$ be an (n, M_i, d_i) code with $\mu(\mathscr{C}_i) \geqslant g_i$, for suitable integers*

$$M_i \geqslant \binom{m+i-1}{i}, \quad d_i \geqslant 7 - 2i, \quad g_i \geqslant 7 - i.$$

Suppose further that $\Delta(\mathscr{C}_1, \mathscr{C}_2) \geqslant 4$. Then for all $j = 1, 2, 3, \ldots$, there exists an $(n + 3j, M', 5)$ code $\mathscr{D}_1^{(j)}$ with $M' \geqslant 2^j m$, $\mu(\mathscr{D}_1^{(j)}) \geqslant g_1$, together with an $(n + 3j, M'', 3)$ code $\mathscr{D}_2^{(j)}$ such that $M'' \geqslant \binom{2^j m}{2}$, $\mu(\mathscr{D}_2^{(j)}) \geqslant g_2$ and $\Delta(\mathscr{D}_1^{(j)}, \mathscr{D}_2^{(j)}) \geqslant 4$.

Proof. Let $\mathscr{D}_1^{(0)} = \mathscr{C}_1$ and $\mathscr{D}_2^{(0)} = \mathscr{C}_2$. For each $j = 1, 2, 3, \ldots$ let us define[8]

$$\mathscr{D}_1^{(j)} = \{\mathscr{D}_1^{(j-1)} \oplus 0 \cdots 0\} \otimes 000 \cup \{\mathscr{D}_1^{(j-1)} \oplus 110 \cdots 0\} \otimes 111,$$

$$\mathscr{D}_2^{(j)} = \{\mathscr{D}_2^{(j-1)} \oplus 0 \cdots 0\} \otimes 000 \cup \{\mathscr{D}_2^{(j-1)} \oplus 10 \cdots 0\} \otimes 110$$
$$\cup \{\mathscr{D}_2^{(j-1)} \oplus 010 \cdots 0\} \otimes 101 \cup \{\mathscr{D}_2^{(j-1)} \oplus 110 \cdots 0\} \otimes 011.$$

It is not hard to verify (see also [22, Chapter 18, Section 7, Theorem 9] that for all $j = 1, 2, \ldots$,

$$\delta(\mathscr{D}_1^{(j)}) \geqslant 5, \quad \delta(\mathscr{D}_2^{(j)}) \geqslant 3 \quad \Delta(\mathscr{D}_1^{(j)}, \mathscr{D}_2^{(j)}) = \Delta(\mathscr{D}_1^{(j-1)}, \mathscr{D}_2^{(j-1)}) = \Delta(\mathscr{C}_1, \mathscr{C}_2) \geqslant 4.$$

[7] This bound can be further optimized. As the result of computer search for special tuples of codes, it turns out that non-adaptive winning strategies with $\mathrm{ch}(\sigma)$ questions, for any such state σ do exist for all $m \geqslant 44$, [8]. Remarkably enough, for all $9 \leqslant m \leqslant 12$, the Golay code [18] yields perfect non-adaptive winning strategies to find an unknown m-bit number when up to three of the answers are mendacious/erroneous.

[8] Given any code $\mathscr{G}$ of length n together with tuples $\boldsymbol{x} = x_1 \cdots x_n \in \{0,1\}^n$ and $\boldsymbol{a} = a_1 a_2 \cdots a_s \in \{0,1\}^s$, we denote by $\{\mathscr{G} \oplus \boldsymbol{x}\} \otimes \boldsymbol{a}$ the code of length $n + s$ whose codewords are obtained by adding $\boldsymbol{x}$ (termwise and modulo 2) to every codeword of $\mathscr{G}$, and then appending the suffix $\boldsymbol{a}$ to the resulting n-tuple.

Moreover for $i=1,2$ we have $\mu(\mathscr{D}_i^{(j)})=\mu(\mathscr{D}_i^{(j-1)}) \geqslant g_i$. Finally,

$$|\mathscr{D}_1^{(j)}| = 2|\mathscr{D}_1^{(j-1)}| = 2^j|\mathscr{D}_1^{(0)}| \geqslant 2^j m,$$

$$|\mathscr{D}_2^{(j)}| = 4|\mathscr{D}_2^{(j-1)}| = 4^j|\mathscr{D}_2^{(0)}| \geqslant 4^j \binom{m+1}{2}$$

$$= \frac{4^j(m^2+m)}{2} > \frac{4^j m^2 - 2^j m}{2} = \binom{2^j m}{2}$$

as required. □

Lemma 5.2. *For all $n \geqslant 19$ there is an (n, M_1, d_1) code $\mathscr{C}_{n,1}$ and an (n, M_2, d_2) code $\mathscr{C}_{n,2}$ such that*

$$M_1 \geqslant m_{n,3}, \quad d_1 \geqslant 5, \quad M_2 \geqslant \binom{m_{n,3}}{2}, \quad d_2 \geqslant 3,$$
$$\mu(\mathscr{C}_{n,1}) \geqslant 6, \quad \mu(\mathscr{C}_{n,2}) \geqslant 5, \quad \Delta(\mathscr{C}_{n,1}, \mathscr{C}_{n,2}) \geqslant 4.$$

Proof. By direct inspection in [6, Table I-A, I-B], for $n=20,21,22$, there exist codes $\mathscr{D}_{n,1}, \mathscr{D}_{n,2}, \mathscr{D}_{n,3}$ such that

(i) $\mathscr{D}_{n,1}$ is an $(n, M_{n,1}, 6)$ code and $w_H(\boldsymbol{x})=6$ for any $\boldsymbol{x} \in D_{n,1}$,
(ii) $\mathscr{D}_{n,2}$ is an $(n, M_{n,2}, 4)$ code and $w_H(\boldsymbol{x})=10$ for any $\boldsymbol{x} \in D_{n,2}$,
(iii) $\mathscr{D}_{n,3}$ is an $(n, M_{n,3}, 4)$ code and $w_H(\boldsymbol{x})=13$ for any $\boldsymbol{x} \in D_{n,3}$.

Moreover,

$$M_{n,1} > \sqrt[3]{6}\, 2^{n/3} + 3 \geqslant m_{n,3}$$

and

$$M_{n,2} + M_{n,3} > \binom{\sqrt[3]{6}\, 2^{n/3} + 4}{2} \geqslant \binom{m_{n,3}+1}{2} > \binom{m_{n,3}}{2}.$$

It is apparent that $\Delta(\mathscr{D}_{n,2}, \mathscr{D}_{n,3}) \geqslant 3$.

Define $\mathscr{C}_{n,1} = \mathscr{D}_{n,1}$ and $\mathscr{C}_{n,2} = \mathscr{D}_{n,2} \cup \mathscr{D}_{n,3}$. Trivially, $\mu(\mathscr{C}_{n,1}) \geqslant 6$ and $\mu(\mathscr{C}_{n,2}) \geqslant 5$. Hence the claim holds for $n=20,21,22$.

For any $n \geqslant 23$, write $n = n' + 3j$ with $n' \in \{20,21,22\}$ and $j \geqslant 1$. Then by Lemma 5.1 there exist an $(n, M', 5)$ code $\mathscr{C}_{n,1}$ with

$$M' \geqslant 2^j m_{n',3} > m_{n'+3j,3} = m_{n,3}$$

and an $(n, M'', 3)$ code $\mathscr{C}_{n,2}$ with

$$M'' \geqslant \binom{2^j m_{n',3}}{2} > \binom{m_{n,3}}{2}$$

such that $\mu(\mathscr{C}_{n,1}) \geqslant 6, \mu(\mathscr{C}_{n,2}) \geqslant 5$ and $\Delta(\mathscr{C}_{n,1}, \mathscr{C}_{n,2}) \geqslant 4$. Hence the desired result holds for all $n \geqslant 20$.

For the remaining case $n=19$, direct inspection in [6, Table I-A, I-B] again yields three codes $\mathscr{D}_{n,i}$ $(i=1,2,3)$ as above, with $M_{n,1}=172>127=m_{19,3}$ and $M_{n,2}+M_{n,3}=8322>8001=\binom{m_{19,3}}{2}$. This concludes the proof. □

Corollary 5.3. *Fix an integer $m\geqslant 99$, and let σ be an arbitrary state of type $(1,m,\binom{m}{2},\binom{m}{3})$. Then there exists a perfect non-adaptive winning strategy $\mathscr{S}$ for σ (in the sense that the number of questions in $\mathscr{S}$ coincides with Berlekamp's lower bound $\mathrm{ch}(\sigma)=q_3(m)-m$).*

Proof. Let $n=\mathrm{ch}(\sigma)$. From the assumption $m\geqslant 99$ by direct inspection, we get $n\geqslant 19$. Lemma 5.2 yields an (n,a_1,d_1) code $\mathscr{D}_1$ with $a_1\geqslant m_{n,3}$, $\mu(\mathscr{D}_1)\geqslant 6$, $d_1\geqslant 5$ together with an (n,a_2,d_2) code $\mathscr{D}_2$ with $a_2\geqslant\binom{m_{n,3}}{2}$, $\mu(\mathscr{D}_2)\geqslant 5$, $d_2\geqslant 3$ satisfying the inequality $\Delta(\mathscr{D}_1,\mathscr{D}_2)\geqslant 4$. By definition, $m\leqslant m_{n,3}$. Pick subcodes $\mathscr{C}_1\subseteq\mathscr{D}_1$ and $\mathscr{C}_2\subseteq\mathscr{D}_2$ such that $|\mathscr{C}_1|=m$ and $|\mathscr{C}_2|=\binom{m}{2}$.Finally let the $(n,1,7)$ code $\mathscr{C}_0$ be defined by $\mathscr{C}_0=\{0\ldots 0\}$. Then the desired conclusion directly follows by Lemma 3.3, using the triplet of codes $\Gamma=(\mathscr{C}_0,\mathscr{C}_1,\mathscr{C}_2)$. □

6. Shrinking the first batch of questions

The problem considered in this section naturally arises from the *asymmetric* nature of the communication between Questioner and Responder. Indeed, in our scenario the forward Questioner-to-Responder channel is *noiseless*, while the feedback channel is *noisy*. In the cooperative model, where Questioner and Responder have agreed on the searching strategy, and lies are replaced by distortions, our results show that error correction can be achieved via the following protocol:

(i) Send m bits over the noisy Responder-to-Questioner channel.
(ii) Over the noiseless feedback channel, send to the Responder the $m-$tuple of bits, as actually received by the Questioner.
(iii) Finally, send to the Questioner a final tip of $q_e(m)-m$ bits, over the noisy channel.

Since in many concrete situations the noiseless feedback channel is much more costly than the forward noisy channel, one can reasonably consider the problem of minimizing the number of feedback bits to be sent during stage (ii). The following problem is especially interesting for us:

To which extent can one decrease the number of bits sent over the noiseless channel, while still keeping to a minimum both the total number of questions and the number of non-adaptive batches of questions?

As we shall see, for every integer $k\geqslant 1$ one can always reduce from m to by $m-k$ the number of questions in the first batch (whence similarly reduce the number of feedback bits over the noiseless channel), for all suitably large m.

Fix an integer $k\geqslant 1$ and let m be a sufficiently large integer. Suppose that the Questioner's first batch of questions only consists of the first $m-k$ queries of Section 4.1.

Then a direct computation shows that the resulting state $\sigma_k = (A_0, A_1, \ldots, A_e)$ is of type

$$\left(2^k, 2^k(m-k), 2^k\binom{m-k}{2}, \ldots, 2^k\binom{m-k}{e}\right)$$

and $\mathrm{ch}(\sigma_k) = q_e(m) - m + k$. For the desired perfect two-round strategy, we must exhibit, for the state σ_k, a non-adaptive winning strategy with $q_e(m) - m + k$ questions. To this purpose, we need the following generalization of Lemma 4.3:

Lemma 6.1. *For any two fixed integers $e, k \geqslant 1$, and for all sufficiently large integers n there exists an e-tuple of codes $\Gamma = (\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_{e-1})$ together with integers $d_i \geqslant 2(e-i)+1$ $(i = 0, 1, \ldots, e-1)$ such that*

(i) *Each $\mathscr{C}_i$ is an $(n+k, 2^k\binom{m_{n,e}-k}{i}, d_i)$ code;*

(ii) *$\Delta(\mathscr{C}_i, \mathscr{C}_j) \geqslant 2e - (i+j) + 1$, (whenever $0 \leqslant i < j \leqslant e-1$.)*

Proof. Let $n' = n - e^2 + k$. First we prove the existence of an $(n', 2^k\binom{m_{n,e}}{e-1}, d')$ code, with $d' = 2e+1$. From Lemma 4.2 together with the well known inequality $e! \leqslant (e+1)^e/2^e$, it follows that, for all sufficiently large n

$$\begin{aligned}
\binom{m_{n,e}-k}{e-1} 2^k &< (m_{n,e})^{e-1} 2^k \\
&< 2^k (\sqrt[e]{e!}\, 2^{n/e} + e)^{e-1} \\
&\leqslant 2^k (e 2^{n/e})^{e-1} \\
&= e^{e-1} 2^{n(e-1)/e + k} \\
&\leqslant \frac{2^{n-e^2+k}}{\sum_{j=0}^{2e}\binom{n-e^2+k}{j}}.
\end{aligned}$$

The existence of the desired $(n', 2^k\binom{m_{n,e}-k}{e-1}, d')$ code follows from Gilbert's Bound. We have proved that, for all sufficiently large n, there exists an $(n-e^2+k,\ 2^k\binom{m_{n,e}-k}{e-1}, d')$ code $\mathscr{C}'$ with $d' \geqslant 2e+1$. Proceeding now as in the proof of Lemma 4.3, we can easily prove the existence of a new e-tuple of codes $\Gamma = (\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_{e-1})$ satisfying both conditions (i) and (ii). This completes the proof. □

The following corollary implies the existence of minimum adaptiveness perfect searching strategies with a first batch of $m-k$, rather than m, questions.

Corollary 6.2. *Fix two integers $e \geqslant 0$, and $k \geqslant 0$. Then for all sufficiently large integers m and for every state σ_k of type $(2^k, (m-k)2^k, \binom{m-k}{2}2^k, \ldots, \binom{m-k}{e}2^k)$ there exists a non-adaptive winning strategy $\mathscr{S}$ such that the number of questions in $\mathscr{S}$ coincides with Berlekamp's lower bound $\mathrm{ch}(\sigma_k) = q_e(m) - m + k$.*

Proof. We can safely assume $e, k \geqslant 1$. Let $n = \mathrm{ch}(\sigma_k)$. By definition, $n \to \infty$ as $m \to \infty$. Lemmas 6.1 and 3.3 yield a non-adaptive winning strategy with n questions for any state of type $(2^k, 2^k(m_{n,e} - k), 2^k\binom{m_{n,e}-k}{2}, \ldots, 2^k\binom{m_{n,e}-k}{e})$. By Definition 4.1, $m \leqslant m_{n,e}$, whence a fortiori, for all sufficiently large m, a non-adaptive winning strategy with n questions exists for any state of type $(2^k, 2^k(m-k), 2^k\binom{m-k}{2}, \ldots, 2^k\binom{m-k}{e})$. □

7. Conclusions and open problems

For all sufficiently large search spaces we have proved the existence of *perfect* e error correcting search strategies where adaptiveness occurs only once. Our results also suggest several interesting problems, as follows:

1. With reference to Section 6, what is the minimum number of questions, $\xi(m, e)$, in the first batch of a two round *perfect* strategy for searching an unknown m-bit number when up to e of the answers are lies?
2. Which sorts of minimally adaptive perfect strategies exist if questions allow the Responder to choose between several (rather than merely two) options, as in [2, 13, 10]?
3. It is of practical interest to extend to $e > 3$ the non-asymptotic results of Section 5.
4. A further line of research deals with the applicability of our methods to various related problems in the area of computing with unreliable tests (e.g., [21]).

Acknowledgements

We thank Vladimir I. Levenshtein for his useful comments and suggestions.

References

[1] M. Aigner, Combinatorial Search, Wiley-Teubner, New York, Stuttgart, 1988.
[2] M. Aigner, Searching with lies, J. Combin. Theory, Ser. A 74 (1995) 43–56.
[3] J.A. Aslam, A. Dhagat, Searching in the presence of linearly bounded errors, Proc. 23rd ACM STOC (1991) 486–493.
[4] E.R. Berlekamp, Block coding for the binary symmetric channel with noiseless, delayless feedback, in: H.B. Mann (Ed.), Error-correcting Codes, Wiley, New York, 1968, pp. 61–88.
[5] R.S. Borgstrom, S. Rao Kosaraju, Comparison-based search in the presence of errors, Proc. 25th ACM STOC (1993) 130–136.
[6] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, A new table of constant weight codes, IEEE Trans. Inform. Theory 36 (1990) 1334–1380.
[7] N. Cesa-Bianchi, Y. Freund, D. Helmbold, M.K. Warmuth, On-line prediction and conversion strategies, Mach. Learning 25 (1996) 71–110.
[8] F. Cicalese, Reliable computation, with unreliable information, Ph.D. Thesis, University of Salerno, 2001.
[9] F. Cicalese, D. Mundici, Optimal binary search with two unreliable tests and minimum adaptiveness, Proc. ESA99, Lecture Notes in Computer Science, Vol. 1643, 1999, pp. 257–266.
[10] F. Cicalese, D. Mundici, Perfect 2-fault tolerant search with minimum adaptiveness, Adv. Appl. Math. 25 (2000) 65–101.
[11] F. Cicalese, D. Mundici, U. Vaccaro, Least adaptive optimal search with unreliable tests, Proc. SWAT2000, Lecture Notes in Computer Science, Vol. 1851, 2000, pp. 547–562.

[12] F. Cicalese, D. Mundici, U. Vaccaro, Rota-Metropolis cubic logic and Ulam–Rényi games, in: H. Crapo, D. Senato (Eds.), Algebraic Combinatorics and Computer Science—A Tribute to Giancarlo Rota, Springer-Verlag, Italia, Milano, 2001, pp. 197–244.
[13] F. Cicalese, U. Vaccaro, Optimal strategies against a liar, Theoret. Comput. Sci. 230 (2000) 167–193.
[14] J. Czyzowicz, D. Mundici, A. Pelc, Ulam's searching game with lies, J. Combin. Theor. Ser. A 52 (1989) 62–76.
[15] A. Dhagat, P. Gacs, P. Winkler, On playing "Twenty Question" with a liar, Proc. 3rd ACM-SIAM SODA (1992) 16–22.
[16] R.L. Dobrushin, Information transmission in a channel with feedback, Theory Probab. Appl. 34 (1958), 367–383 (reprinted in: D. Slepian (Ed.), Key Papers in the Development of Information Theory, IEEE Press, New York, 1974).
[17] D.Z. Du, F.K. Hwang, Combinatorial Group Testing and its Applications, World Scientific, Singapore, 1993.
[18] M.J.E. Golay, Notes on digital coding, Proc. IEEE 37 (1949) 657.
[19] R. Hill, Searching with lies, in: P. Rowlinson (Ed.), Surveys in Combinatorics, Cambridge University Press, Cambridge, 1995, pp. 41–70.
[20] R. Karp, ISIT'98 Plenary Lecture Report: Variations on the theme of 'Twenty Questions', IEEE Information Theory Society Newsletter Vol. 49 No.1 March 1999.
[21] C. Kenyon, A.C. Yao, On evaluating boolean functions with unreliable tests, Internat. J. Found. Comput. Sci. 1 (1990) 1–10.
[22] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[23] D. Mundici, Ulam's game, Łukasiewicz logic and AF C^*-algebras, Fund. Inform. 18 (1993) 151–161.
[24] D. Mundici, A. Trombetta, Optimal comparison strategies in Ulam's searching game with two errors, Theoret. Comput. Sci. 182 (1997) 217–232.
[25] S. Muthukrishnan, On optimal strategies for searching in presence of errors, Proc. 5th ACM-SIAM SODA (1994) 680–689.
[26] A. Negro, M. Sereno, Ulam's searching game with three lies, Adv. Appl. Math. 13 (1992) 404–428.
[27] A. Pelc, Solution of Ulam's problem on searching with a lie, J. Combin. Theory, Ser. A 44 (1987) 129–142.
[28] A. Pelc, Weakly adaptive comparison searching, Theoret. Comput. Sci. 66 (1989) 105–111.
[29] A. Pelc, Searching with permanently faulty tests, Ars Combin. 38 (1994) 65–76.
[30] A. Pelc, Search games with errors—fifty years of coping with liars, preprint, 2000.
[31] A. Rényi, On a problem of information theory, MTA Mat. Kut. Int. Kozl. 6B (1961) 505–516.
[32] A. Rényi, Napló az információelméletről, Gondolat, Budapest, 1976. (English translation: A Diary on Information Theory, Wiley, New York, 1984.)
[33] R.L. Rivest, A.R. Meyer, D.J. Kleitman, K. Winklmann, J. Spencer, Coping with errors in binary search procedures, Proc. 10th ACM STOC (1978) 227–232.
[34] J. Spencer, Ulam's searching game with a fixed number of lies, Theoret. Comput. Sci. 95 (1992) 307–321.
[35] J. Spencer, P. Winkler, Three thresholds for a liar, Combin. Probab. Comput. 1 (1992) 81–93.
[36] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. 24 (1973) 88–96.
[37] S.M. Ulam, Adventures of a Mathematician, Scribner's, New York, 1976.
[38] J. von Neumann, Probabilistic logics and the synthesis of reliable organisms from unreliable components, in: C.E. Shannon, J. McCarthy (Eds.), Automata Studies, Princeton University Press, Princeton, NJ, 1956, pp. 43–98.
[39] V.A. Zinoviev, V.K. Leontiev, The non-existence of perfect codes over Galois fields, Probab. Control Inform. Theory 2 (1973) 123–132.
[40] V.A. Zinoviev, G.L. Katsman, Universal code families, Inform. Theory Coding Theory 29 (2) (1993) 95–100.