Information Sciences 179 (2009) 3645–3658

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Two cooperative versions of the Guessing Secrets problem

G. Sergioli [b], A. Ledda [b], F. Paoli [b,*], R. Giuntini [b], T. Kowalski [b], F. Montagna [a], H. Freytes [b,c], C. Marini [a]

[a] Dept. of Mathematics, University of Siena, Italy
[b] Dept. of Education, University of Cagliari, 09123 Cagliari, Italy
[c] Consejo Nacional de Investigaciones Cientificas y Tecnicas, Instituto Argentino de Matematica, Argentina

ARTICLE INFO

Article history:
Received 12 December 2008
Received in revised form 28 May 2009
Accepted 2 June 2009

Keywords:
Guessing Secrets problem
Ulam game
Fuzzy logic
Game-theoretic semantics

ABSTRACT

We investigate two cooperative variants (with and without lies) of the Guessing Secrets problem, introduced in [L. Chung, R. Graham, F.T. Leighton, Guessing secrets, Electronic Journal of Combinatorics 8 (2001)] in the attempt to model an interactive situation arising in the World Wide Web, in relation to the efficient delivery of Internet content. After placing bounds on the cardinality of the smallest set of questions needed to win the game, we establish that the algebra of all the states of knowledge induced by any designated game is a pseudocomplemented lattice. In particular, its join semilattice reduct is embeddable into the corresponding reduct of the Boolean algebra $\mathbf{2}^{N-1}$, where N is the cardinality of the search space.

1. Introduction

The Guessing Secrets problem (GSP) we will be concerned with was introduced in [3] in an attempt to model an interactive situation arising in the World Wide Web in relation to the efficient delivery of the Internet content, especially to machines using more than one IP address. A home computer with only one link to the Internet would typically have only one IP address at any given time. Even if dynamically allocated, such an address would be relatively easy to determine. However, computers in different environments, for instance in large corporations, tend to have two or more addresses at the same time, for security and other reasons (cf. [12,15]).

Suppose that a client computer **A** has $S = \{a_1, \ldots, a_n\}$ IP addresses in a nameserver **N**, and suppose it switches from one to another with an unknown probability distribution. The question then arises, how much one can learn about that probability distribution from the nameserver **N** by asking binary questions, and how fast such queries can be carried out.

The IP addresses in S can be viewed as 'secrets' to be guessed. The probability distribution $\mathrm{p}(a_i)$, for $a_i \in S$, is then induced by the number of times **A** connects to the Internet via the IP address a_i. To be precise, if $\mu(a_i)$ is the number of times **A** connected to the Internet with the IP address a_i, and k is the total number of times **A** connected to the Internet, then

$$\mathrm{p}(a_i) = \frac{\mu(a_i)}{k},$$

as modelled in our probabilistic version of the GSP.

In an abstract setting, the Guessing Secrets problem can be formulated as follows: Bob is trying to determine, within a search space Ω of N objects, say natural numbers, the identity of $j \geqslant 2$ 'secrets', which are known to his opponent Alice

* Corresponding author.
E-mail address: paoli@unica.it (F. Paoli).

0020-0255/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.06.014

but unknown to him. Bob is allowed to ask Alice binary 'yes–no' questions of the form 'Is your secret in X?' (for $X \subset \Omega$). To such questions Alice is obliged to respond truthfully, however, she is permitted to choose adversarially (i.e. in such a way as to prevent Bob from discovering the secrets) which of the j secrets her answer refers to. For example, if $\Omega = \{1, 2, 3, 4\}$ and the secrets are 1 and 2, Alice must answer 'yes' to the question 'Is your secret smaller than 3?', but she may answer either way to the question 'Is your secret odd?', for she might refer either to 1 (which is odd) or to 2 (which is not). The game is a generalisation of the familiar Twenty Questions game, which corresponds to the special case $j = 1$.

Although the structure of the problem implies that Bob can never be sure that he has discovered the secrets (a winning strategy is always available to Alice), several optimal strategies to maximise the amount of information and to select questions have been devised at least for the case $j = 2$; the corresponding algorithms run in polynomial time. The problem becomes intractable for $j > 2$ ([1,4,9,10], but also see [14]). Further applications of the problem include such disparate tasks as separating systems into smaller units, diagnosing technical problems, protecting data from unauthorised reproduction, authenticating ownership claims.

An interesting variant of the GSP was introduced in [7]. The authors remark that, in some situations where a client computer can use any one of several different IP addresses, the address used by the client at any moment could be chosen at random according to some particular probability distribution. This suggests a version of the GSP in which Alice does not choose adversarially the secret to which she refers at each move of the game, but rather she selects it at random.

In this paper we introduce two variants (with and without lies) of the GSP, which aim at modelling certain aspects of the transmission process of uncertain information—namely, situations where the transmitter does not have a perfect knowledge of the data which the receiver is enquiring about (cf. [18]).

In the variant without lies of our *cooperative* GSP, like in the familiar Twenty Question game, the respondent (Alice) is not free to select any strategy: her truthful answers are completely determined by the structure of the asked question. In game-theoretical terms, therefore, it can be described as a single player game. Bob's aim is finding out a secret number $n \in \Omega$. Alice is ready to cooperate with Bob's search, but the secret number is now unknown to her, too. Her knowledge of n exceeds Bob's only in that she is assumed to have performed a given number of *measurements* on Ω, each of which returned as an outcome a member of Ω. We assume, for the sake of simplicity, that Bob knows the total number of measurements performed by Alice, and of course we assume that the same member of Ω can be the outcome of several different measurements. The best Alice can do to help Bob, therefore, is to provide him with information about the *relative frequencies* of members of the search space in the set of measurements she has performed. Since the only information source available to Bob is given by Alice's answers to his own yes–no questions, in general he will not succeed in guessing the secret number n; so, he must fall back on the more modest project of reconstructing the probability distribution induced by the measurements Alice has performed.

The paper is structured as follows: in Section 2 we introduce our cooperative variant of the game and investigate its properties; the main result of the section states that the number of questions to be asked in order to solve the game is bounded above by a polynomial function whose arguments are the cardinality of the search space and the number of secrets. Section 3 contains some basic observations on the structure of a cooperative Guessing Secrets problem where the respondent is allowed to *lie* a certain number of times. Finally, in Section 4 we investigate some general properties of the algebra of all the states of knowledge induced by games on a fixed search space, subsequently focusing on the algebra of states of knowledge arising from a single designated game.

2. A cooperative version of the Guessing Secrets problem

In more detail, the game develops according to the following pattern.

Two players, Alice and Bob, agree on a *search space* consisting of a nonempty finite set $\Omega = \{1, \ldots, 2^M\}$ of consecutive natural numbers, whose cardinality we assume, for the sake of simplicity, to be a power of 2. They also agree that Alice can draw j *secrets* ($1 \leqslant j \leqslant 2^{M-1}$) out of Ω (this restriction on j is warranted by the assumption, which is commonplace in the GSP, that j be 'small' w.r.t. the cardinality of the search space). So, Alice knows the identity of the secrets in $S = \{a_1, \ldots, a_j\}$, while Bob does not. Moreover, each number $n \in \Omega$ is supposed to have a *multiplicity* $\mu(n)$, which is a non-negative integer s.t. $\mu(n) > 0$ for $n \in S$, while $\mu(n) = 0$ for $n \in \Omega - S$. Bob's goal in the game is guessing as quickly as possible the identity of each member a_i of S, together with its respective multiplicity $\mu(a_i)$, by asking binary yes–no questions to Alice. As usual, such questions can be formally identified with nonempty subsets $X \subset \Omega$. Alice's answer to X, though, will not be 'yes' or 'no'. Rather, it will be a rational number in between 0 and 1, namely

$$\frac{\sum_{n \in X} \mu(n)}{\sum_{i \leqslant j} \mu(a_i)}.$$

Note that, for $j = 1$, i.e. if all the measurements taken by Alice yielded the same output,[1] we get the Twenty Questions game as a special case.

We now proceed with a more formal description of the game.

[1] Which, for all we know, may not coincide with the secret number to be guessed, if Alice consistently drew the same *wrong* number.

Definition 1. A *game* is an ordered triple $\Gamma = \langle \Omega, S, \mu \rangle$, where:

- $\Omega = \{1, \ldots, 2^M\}$ (the *search space*) is the set of the first 2^M positive integers, for some positive integer M;
- $S = \{a_1, \ldots, a_j\}$ (the *set of secrets*) is a proper subset of Ω s.t. $1 \leqslant j \leqslant 2^{M-1}$;
- $\mu : \Omega \to \mathbb{N}$ is a function (called a *measure* on Ω) such that $\mu(a_i) > 0$ for $a_i \in S$, while $\mu(n) = 0$ for $n \in \Omega - S$.

Intuitively, $\mu(a_i)$ indicates how many times a_i occurred in Alice's measurements. Unless specified otherwise, we assume that Γ is arbitrary but fixed.

Definition 2. A *μ-probability* on Ω is a function $\mathrm{p}_\mu : \Omega \to [0,1] \cap \mathbb{Q}$ such that

$$\mathrm{p}_\mu(n) = \frac{\mu(n)}{\sum_{i \leqslant j} \mu(a_i)}.$$

To attain his goal, Bobby asks questions to Alice. Like in the GSP,

Definition 3. A *question* for $\Gamma = \langle \Omega, S, \mu \rangle$ is a nonempty subset $X \subset \Omega$.

For instance, the question:

Is the number odd?

can be identified with the set of odd numbers $\{1, 3, \ldots, 2^M - 1\}$ in Ω.

Definition 4. An *answer* is the output of a function $\sigma : \mathscr{P}(\Omega) \to [0,1] \cap \mathbb{Q}$ defined as follows:

$$\sigma(X) = \sum_{n \in X} \mathrm{p}_\mu(n).$$

Definition 5. A *match* is an ordered pair $\mathscr{M} = \langle \Gamma, Q \rangle$, where Γ is a game and Q is a set of questions for Γ.

In order to get a better grip of the preceding definitions, let us examine the following

Example 6. Let $\Omega = \{1,2,3,4,5,6,7,8\}$ and let $\mu(1) = 2$, $\mu(2) = 1$, $\mu(4) = 3$, $\mu(5) = 1$, and $\mu(n) = 0$ for $n \in \{3,6,7,8\}$. In other words, Alice took seven draws (measurements), which yielded the numbers 2 and 5 once, the number 1 twice and the number 4 three times. Bob's question 'Is the secret number odd?' corresponds to $X_{odd} = \{1,3,5,7\}$. Consequently, Alice's answer to X will be:

$$\sigma(X_{odd}) = \mathrm{p}_\mu(1) + \mathrm{p}_\mu(3) + \mathrm{p}_\mu(5) + \mathrm{p}_\mu(7) = \frac{2}{7} + 0 + \frac{1}{7} + 0 = \frac{3}{7}.$$

Let us now reflect for a while on the possible courses taken by a cooperative GSP match. Like in the Twenty Questions game, the respondent (Alice) plays no role in the game, i.e. it is not up to her to select a strategy over another: all she has to do is to answer truthfully to Bob's questions. As for Bob, the best strategy available to him consists in: (i) halving the search space each time; (ii) following an adaptive strategy which changes according as the previous answer given by Alice allows him to restrict his search on X (e.g. if X is the first question and $\sigma(X) = 1$) or on $\Omega - X$ (e.g. if X is the first question and $\sigma(X) = 0$), or else it forces him to carry out his search on *both* subsets.

This simple observation leads us to associate to each cooperative GSP a *labelled perfect rooted binary tree* [8], whose nodes are labelled by subsets of Ω. The next definitions provide the necessary ingredients.

Definition 7. If $X, Y \subseteq \Omega$, Y is called a *halving* of X if $Y \subset X$ and $| Y | = \frac{|X|}{2}$.

Definition 8. A set of questions Q is called *normal* if the following conditions are satisfied:

- Each of its members has at most one halving in the set;
- If $X, Y \in Q$ and Y ($| Y | \geqslant 2$) is a halving of X s.t. $\sigma(X - Y) = 0$, then Y has a halving in Q and no proper subset of $X - Y$ belongs to Q;
- If $X, Y \in Q$ and Y ($| Y | \geqslant 2$) is a halving of X s.t. $\sigma(Y) = 0$, then $X - Y$ has a halving in Q and no proper subset of Y belongs to Q;
- If $X, Y \in Q$ and Y ($| Y | \geqslant 2$) is a halving of X s.t. $0 < \sigma(Y), \sigma(X - Y)$, then both Y and $X - Y$ have halvings in Q.

A match is called *normal* iff its set of questions is such.

The preceding definition ensures that the next concept is well-defined.

Definition 9. Given a normal match $\mathscr{M} = \langle \Gamma, Q \rangle$, where Q includes exactly one halving of Ω, the *GSP-tree* associated to $\mathscr{M}$ is constructed as follows:

- Its root is labelled by Ω;
- If the node α is labelled by X and $Y \in Q$ is a halving of X s.t. $\sigma(Y) = 0$ ($\sigma(X - Y) = 0$) then α has a single child α', labelled by $X - Y$ (Y);
- If the node α is labelled by X and $Y \in Q$ is a halving of X s.t. $0 < \sigma(Y), \sigma(X - Y)$, then α has two children α' and α'', respectively labelled by Y and $X - Y$.

Definition 10. An answer $\sigma(X)$ is called *Boolean* iff there exists $Y \subseteq \Omega$ s.t.:

- X is a halving of Y;
- Either $\sigma(X) = 0$ or $\sigma(Y - X) = 0$.

Lemma 11. *If $\mathscr{M} = \langle \Gamma, Q \rangle$ is a normal match and $S = \{a_1, \ldots, a_j\}$ is the set of secrets of Γ, the number of nonboolean answers given by Alice is equal to $j - 1$.*

Proof. In a GSP-tree, every node will have just one child unless it arises from a nonboolean answer. Every nonboolean answer adds one fork: the number of nonboolean answers in the match is equal to the number of forks minus 1. When the solution has been reached, the number of forks is equal to the number of the leaves, i.e. $| S | = j$. It follows that the number of nonboolean answers is $j - 1$. □

Corollary 12. *All answers given by Alice are Boolean iff there exists a single secret $a_i \in \Omega$ s.t. $\mathrm{p}_\mu(a_i) = 1$.*

Lemma 11 also implies, given our restriction on j, that at least an answer given by Alice must be Boolean.

By Lemma 11, if $j = 1$, i.e. in the special case of the Twenty Questions game, our tree becomes a chain. By the same Lemma, moreover:

Lemma 13. *For any normal match $\mathscr{M}$, the GSP-tree associated with $\mathscr{M}$ contains $j - 1$ nodes with two children, where j is the number of secrets.*

Henceforth, when we say that a given GSP-tree is associated with the game Γ whenever it is associated with at least one normal match $\mathscr{M} = \langle \Gamma, Q \rangle$; by a GSP-tree *tout court*, we will mean a GSP-tree associated with some game Γ.

Let us now introduce the notion of maximal GSP-tree, which will be extremely useful in what follows:

Definition 14. A GSP-tree is said to be *maximal* iff the depth of each node with a single child is greater or equal than the depth of any node with two children.

Intuitively, a maximal GSP-tree is a GSP-tree where all the forks are located in the upper part of the tree; no node with a single child can be strictly closer to the root than a node with two children. The following two lemmas are immediate consequences of the definitions:

Lemma 15. *Let Γ be a game; all maximal GSP-trees associated with Γ have the same size.*

Proof. By Lemma 13 and direct inspection of the construction of a maximal GSP-tree. □

Lemma 16. *For any game $\Gamma = \langle \Omega, S, \mu \rangle$, where S has cardinality j, there is a maximal GSP-tree associated to Γ.*

Proof. Induction on j. □

In virtue of Lemma 15, for the following considerations we may disregard as inessential the differences between any two maximal GSP-trees associated with a given game Γ. Therefore, from now on, if the GSP-trees associated with the normal matches

$$\mathscr{M}_1 = \langle \Gamma, Q_1 \rangle, \ldots, \mathscr{M}_p = \langle \Gamma, Q_p \rangle$$

are all maximal, we will call any one of them *the maximal GSP-tree* associated to Γ. The next Example will help to clarify all the notions introduced so far.

Example 17. Let $\Gamma = \langle \Omega, S, \mu \rangle$, where $\Omega = \{1, \ldots, 16\}$, $S = \{1, 5, 6, 8, 12, 13, 14, 16\}$, $\mu(n) = 1$ for $n \in \{1, 6, 8, 13, 14, 16\}$, and $\mu(5) = \mu(12) = 2$. A possible non-maximal GSP-tree associated with Γ is depicted in Fig. 2.1, while the maximal GSP-tree associated with Γ is in Fig. 2.2.

We are now going to investigate a fundamental question: is there any upper bound to the number of questions which Bob must ask in a game $\Gamma = \langle \Omega, S, \mu \rangle$ in order to retrieve the probability distribution induced by μ? Let us first tackle this problem in the special case of Example 17. It is clear from Fig. 2.2 that the number of steps required to discover the probability distribution is equal to 15. We can calculate this number considering every branch of the tree as a separate Twenty Questions game. For instance, we can decompose the tree in the following eight linearly ordered subsets (here we will not distinguish between the nodes and their labels):

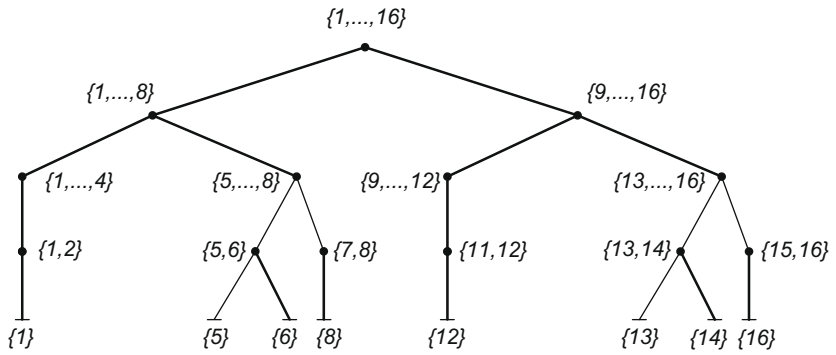


Fig. 2.1. A non-maximal GSP-tree associated with the game of Example 17.

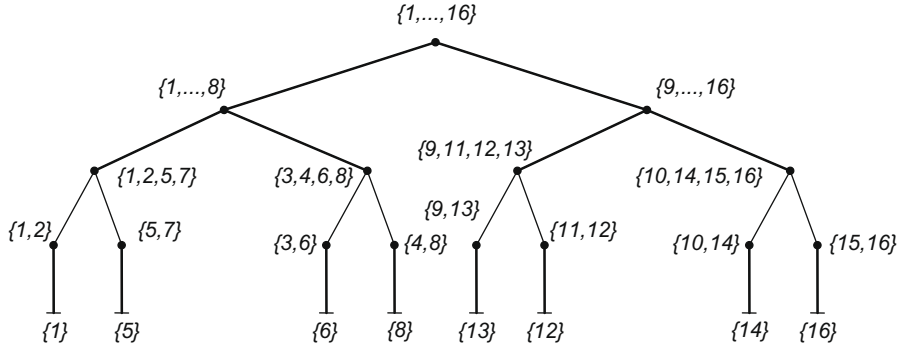


Fig. 2.2. The maximal GSP-tree associated with the game of the same Example.

$$b_1 = \left\{ \begin{matrix} \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}, \\ \{1,2,3,4,5,6,7,8\},\{1,2\},\{1\} \end{matrix} \right\}$$
$$b_2 = \{\{3,4,6,8\},\{3,6\},\{6\}\}$$
$$b_3 = \{\{5,7\},\{5\}\}$$
$$b_4 = \{\{4,8\},\{8\}\}$$
$$b_5 = \{\{9,11,12,13\},\{9,13\},\{13\}\}$$
$$b_6 = \{\{10,14,15,16\},\{15,16\},\{16\}\}$$
$$b_7 = \{\{11,12\},\{12\}\}$$
$$b_8 = \{\{10,14\},\{14\}\}$$

Notice that, for any i,j, $b_i \cap b_j = \emptyset$. Let C_i denote the cardinality of the set labelling the minimal node of the i-th linearly ordered subset

$$C_1 = 4, \quad C_2 = 3, \quad C_3 = 2, \quad C_4 = 2$$
$$C_5 = 3, \quad C_6 = 3, \quad C_7 = 2, \quad C_8 = 2.$$

It is clear that the size of the GSP-tree is precisely the sum of the nodes of the linearly ordered subsets, which is exactly $\sum_i^n \log_2 C_i$. In fact, $15 = \sum_{i=1}^{8} \log_2 C_i$. This particular example can be generalised as follows:

Lemma 18. *For any game $\Gamma = \langle \Omega, S, \mu \rangle$, the cardinality of the smallest normal set of questions Q which, in the worst possible case, Bob must ask to retrieve the probability distribution induced by μ is $s - l$, where s is the size of the GSP-tree associated with Q, and l is the number of its leaves.*

Proof. Just observe that every question in the GSP-tree associated to Q is represented by a node with at least one child. It is also worth to observe that, for a given question X_i, the number of its children only depends on whether $\sigma(X_i)$ is Boolean or not, a fact which does not depend on the values of the measurement function for the members of X_i.

The previous Lemma considerably simplifies our task, for we can reduce the study of the length of any normal match to an investigation of its associated GSP-tree. The luckiest case, of course, occurs when $j = 1$, i.e. when all the answers are Boolean. In that case, any GSP-tree associated with the game is linearly ordered, and $\log_2 2^M = M$ questions will suffice. What happens, instead, when $j > 1$?

Lemma 19. *Let Γ be a game, and let T_m be the maximal GSP-tree associated to Γ. Then*

$$Size(T_m) = \max\{Size(T) : T \text{is aGSP-tree associated with } \Gamma\}.$$

Proof. $\Leftarrow$ Let T be the GSP-tree associated to Γ having the highest size, say s, and suppose that T is not maximal. Thus, by Definition 14, there are nodes α, with two children, and β, with one child, s.t. the depth of α is greater than the depth of β. By Lemmas 15 and 16 we can associate to Γ its maximal GSP-tree T_m, which by definition must have a node β' with two children and with the same depth as β. Consider, now, the subtree T' of T with root β and the subtree T'_m of T_m with root β'. T' and T'_m have the same depth, but the size of T' is greater than the size of T'_m. This implies that the size of T_m is greater than the size of T, against the hypothesis.

$\Rightarrow$ Let T_m be the maximal GSP-tree associated to Γ, with size s_m. Suppose that there exists a non-maximal GSP-tree T associated to Γ with size $s > s_m$. Since T and T_m are GSP-trees associated to Γ, by Lemma 13 they must have the same number $j-1$ of nodes with two children. Let h be the highest depth of a node with two children in T_m. Thus, the only way to obtain from T_m another GSP-tree with $j-1$ nodes with two children and size $s > s_m$ is to replace a node with one child with depth $h' < h$ by a node with two children, which is impossible by Definition 14. □

We now can achieve a result concerning the number of questions Bob has to ask to solve the problem. If he asks a normal set of questions, the number of nonboolean answers he will receive will depend neither on his playing strategy nor on luck, but just on the structure of the game (more precisely, on the number of secrets). However, the earlier the nonboolean answers show up in the game, the greater the number of questions he will need to solve the problem. The next Lemma considers the worst case scenario: the case in which the GSP-tree associated with his set of questions is maximal.

Theorem 20. *For any game $\Gamma = \langle \Omega, S, \mu\rangle$, with $|\Omega| = 2^M$ and $|S| = j$, the cardinality of the smallest normal set of questions Q which Bob must ask to retrieve the probability distribution induced by μ is bounded above by*

$$B_M = 2^P(M-P+1) + \left(j - 2^P\right)(M-P-1) - 1$$

where 2^P is the smallest power of 2 which is greater or equal than j.

Proof. By Lemmas 19 and 18, to get an upper bound it is sufficient to determine the number $s-l$, where s is the size of the maximal GSP-tree associated with Γ and l is the number of its leaves. We will prove the theorem by induction on M.

($M = 1$). In this case, necessarily $j = 2^P = 1$. Then $B_1 = 1$, as expected.

($M = N+1$). Rewriting the formula for the case at issue, we must prove that:

$$B_{N+1} = 2^P(N-P+2) + \left(j - 2^P\right)(N-P) - 1.$$

However,

$$B_{N+1} = 2^P(N-P+1) + 2^P + \left(j - 2^P\right)(N-P-1) + j - 2^P - 1 = B_N + j \tag{1}$$

This is the expected result: in passing from the maximal GSP-tree T_m associated with $\Gamma = \langle \Omega, S, \mu\rangle$, with $|\Omega| = 2^N$, to the maximal GSP-tree T'_m associated with $\Gamma' = \langle \Omega', S', \mu'\rangle$, with $|\Omega'| = 2^{N+1}$ and $|S'| = |S| = j$, the number of nodes with two children cannot increase, whence the size T'_m will exceed the size of T_m only by the number of leaves of T_m, each of which must have exactly one child in T'_m. By a property of binary trees, however, the number of such leaves exceeds by 1 the number of nodes with two children – i.e. it is exactly j. □

3. Cooperative GSP with lies

Ulam game is a generalisation of the Twenty Questions game whereby the respondent is allowed to lie at most l times (where l is a fixed number). A copious literature on the game is by now available (see e.g. [2,5,6,11,16,17]). A logical interpretation of Ulam game has been suggested in [13].

In this section, we introduce a common abstraction of Ulam game and the cooperative GSP. Unlike the game without lies, this *cooperative GSP with lies* is not a single player game, for Alice is supposed to select her answers adversarially—in this sense, both players are implementing their own strategies.

We will confine ourselves to an informal and rather sketchy description of the game. The strategy we devise here for Bob (not necessarily optimal) consists in reducing the present game to the game without lies, and then solving it by means of the strategy described before.

Suppose that Alice is allowed to lie l times. Bob will repeat his first question $j_1 = 2l+1$ times. Suppose that Alice lies m_1 times ($0 \leqslant m_1 \leqslant l$); Bob will receive the same answer at least $l+1$ times (if $m_1 = l$) and at most $2l+1$ times (if $m_1 = 0$). We show below how the number of repeats of the same answer Bob received can lead him to guess m_1. Thus, Bob will repeat his

second question $j_2 = 2(l - m_1)$ times, and so on. By A^i we will denote the multiset of j_i answers to the j_i formulations of the i-th question.

Now, Bob considers the multiset $A^1 = \{\sigma_1(X_1), \ldots, \sigma_{j_1}(X_1)\}$ associated to the j_1 repetitions of the first question, and takes the set Σ^1 of all possible combinations of $l+1$ elements of A^1 without repetitions; this means that $\sigma_m(X_1)$ and $\sigma_n(X_1)$ may occur in the same combination even if $\sigma_m(X_1) = \sigma_n(X_1)$, but provided that $n \neq m$. The cardinality of Σ^1 is the number of combinations without repetitions of length $l+1$ on a set with $j_1 = 2l+1$ elements, namely $\frac{(j_1)!}{(l+1)!\ l!}$. We will also need the following generalisation of the Kronecker delta function:

Definition 21. $\Delta : \Sigma^1 \to \{0,1\}$ is defined as follows:

$$\Delta(\{x_1, \ldots, x_{l+1}\}) = \prod_{i=1}^{N} \{\delta_i(x_j, x_k) : x_j, x_k \in \{x_1, \ldots, x_{l+1}\}, j \neq k\},$$

where δ is the Kronecker delta and $N = \frac{(l+1)!}{2((l-1)!)}$.

Indeed, Δ acts as a generalised Kronecker delta. For any $\{x_1, \ldots, x_{l+1}\} \in \Sigma^1$, we can see that:

$$\Delta(\{x_1, \ldots, x_{l+1}\}) = \begin{cases} 1 & \text{if } x_1 = \ldots = x_{l+1} \\ 0 & \text{otherwise} \end{cases}$$

Then, if $\Delta(\{x_1, \ldots, x_{l+1}\}) = 1$, where $x_1 = \ldots = x_{l+1} = \sigma_i(X_1)$, Bob knows that $\sigma_i(X_1)$ is the right answer.

If d is the number of elements of Σ^1 for which the function Δ outputs 0, Bobby can now infer the number $m_1 \leqslant l$ of times Alice has lied on the first question:

Lemma 22. *The number $m_1 \leqslant l$ of falsified answers follows from the equation*

$$\bar{m} \cdot (\overline{m} - 1) \cdot \ldots \cdot (\bar{m} - k + 1) = k! \left[\binom{t}{k} - d \right]$$

where $t = 2l+1$, $k = l+1$ and $\bar{m} = t - m_1$. Such an equation has exactly one solution in $\mathbb{N}$.

Proof. The number d of $\{x_1, \ldots, x_{l+1}\} \in \Sigma^1$ such that $\Delta(\{x_1, \ldots, x_{l+1}\}) = 0$ is equal to

$$\binom{t}{k} - \binom{t - m_1}{k}$$

Thus,

$$\frac{(t - m_1)!}{k!(t - m_1 - k)!}$$
$$= \frac{(t - m_1) \cdot (t - m_1 - 1) \cdot \ldots \cdot (t - m_1 - k + 1) \cdot (t - m_1 - k)!}{k!(t - m_1 - k)!} = \binom{t}{k} - d \quad \square$$

Now Bob has to cope with the second question. He knows that, at the moment, Alice can lie only $l - m_1$ times. He applies again the procedure used in the first question, and so on for the remaining steps. He is, consequently, able to apply the strategy he would apply for the case without lies.

Corollary 23. *The number of questions required to solve a cooperative GSP with l lies, over a search space with 2^M elements, lies in between $M + j_1 - 1$ and $(2^M - 1)j_1$.*

Proof. The number of question required to solve a lie-free cooperative GSP is at best M and at worst $2^M - 1$. Here, on the other hand, the best case scenario is the one in which Alice uses all available lies as answer to the first question, in which case Bob will repeat the first question $2l+1$ times and each one of the remaining $M-1$ questions exactly once, for an overall $2l + 1 + M - 1 = M + j_1 - 1$ questions. The worst case scenario is the one in which Alice uses all available lies as answer to the last question, in which case Bob has to repeat each question $j_1 = 2l+1$ times). The total number of questions, in this case, will be $(2^M - 1)j_1$. $\square$

One may wonder if it is possible to express the number of questions required to solve a cooperative GSP with l lies, over a search space with cardinality 2^M and with j secrets, as a function of the number of steps required to solve the corresponding GSP without lies. The next lemma gives the answer.

Lemma 24. *If $\Gamma = \langle \Omega, S, \mu \rangle$ is a cooperative GSP without lies, solvable in α steps, the number of steps required to solve Γ when l lies are permitted is given by*

$$j_1(\alpha) - 2m_1(\alpha - 1) - \ldots - 2m_{\alpha - 1}$$

where m_i is the number of answers falsified by Alice at each question X_i.

Proof. Suppose that Alice is allowed to lie l times. Bob will repeat his first question $j_1 = 2l+1$ times. Suppose further that Alice lies $m_1 \leqslant l$ times. According to the previously described strategy, Bob can retrieve m_1 from the number of repeat occurrences of the same answer he received. So, Bob will repeat his second question $j_2 = 2(l-m_1)$ times:

$$
\begin{array}{ccccc}
X_1 & & X_2 & & X_3 \\
\vdots & & \vdots & & \vdots \\
m_1 \text{ lies} & & m_2 \text{ lies} & & m_3 \text{ lies} \\
\vdots & & \vdots & & \\
2l+1 \text{ rep. of } X_1 & & 2(l-m_1)+1 \text{ rep. of } X_2 & & 2(l-m_1-m_2)+1 \text{ rep. of } X_3 \\
\ldots & & X_\alpha & & \\
 & & \vdots & & \\
\vdots & & m_\alpha \text{ lies} & & \\
 & & \vdots & & \\
\ldots & & 2(l-m_1-m_2-\ldots-m_{\alpha-1})+1 \text{ rep. of } X_\alpha & &
\end{array}
$$

The total number of steps will be:

$$
\begin{aligned}
&[2l+1] + [2l+1-2m_1] + [2l+1-2(m_1+m_2)] + \ldots \\
&[2l+1-2(m_1+m_2+\ldots+m_{\alpha-1})] = \\
&(2l+1)\alpha - 2m_1(\alpha-1) - 2m_2(\alpha-2) - \ldots - 2m_{\alpha-1} \quad \square
\end{aligned}
$$

4. The algebra of states of knowledge

In the present section, we revert to the game without lies and introduce a further restriction on the type of questions which may permissibly be asked by Bob during the game. Taking up a suggestion by Pelc [16], we identify questions not with arbitrary nonempty subsets of the search space Ω, but rather with special *intervals* therein. This leads to the following

Definition 25. Let $\Gamma = \langle \Omega, S, \mu \rangle$ be a game. The notion of *permissible question* for Γ is inductively defined as follows:

- Ω is a permissible question;
- If X is a permissible question and Y is an initial or final subinterval of X, then Y is a permissible question.

This limitation yields an obvious advantage in the representation of Bob's states of knowledge in his search for the solution of the game, which can now be defined as follows:

Definition 26. A *state of knowledge* (sometimes simply: *knowledge state* or *state*) for the game $\Gamma = \langle \Omega, S, \mu \rangle$, where $\Omega = \{1, \ldots, N\}$ and $S = \{a_1, \ldots, a_n\}$, is a finite sequence

$$K = \langle \langle u_1, k_1 \rangle, \ldots, \langle u_m, k_m \rangle \rangle$$

of pairs of natural numbers, s.t. $u_1 < u_2 < \ldots < u_m = N$, and $\sum_{i=1}^{m} k_i = \sum_{j=1}^{n} \mu(a_j)$.

The information coded by K is: there are k_1 secrets in the interval $[1, u_1]$, k_2 secrets in the interval $(u_1, u_2], \ldots, k_m$ secrets in the interval $(u_{m-1}, N]$.

Example 27. The states

$$
\begin{aligned}
K &= \langle \langle 2,2 \rangle, \langle 5,1 \rangle, \langle 7,1 \rangle, \langle 12,0 \rangle, \langle 16,2 \rangle \rangle \\
K' &= \langle \langle 3,2 \rangle, \langle 6,1 \rangle, \langle 7,1 \rangle, \langle 12,0 \rangle, \langle 14,1 \rangle, \langle 15,0 \rangle, \langle 16,1 \rangle \rangle
\end{aligned}
$$

are depicted in Figs. 4.1 and 4.2.

Let $\mathscr{K}^{\Omega}$ be the set of all knowledge states arising from all possible games with a fixed search space Ω. We now want to endow the set $\mathscr{K}^{\Omega}$ with some structure. First of all, we want to order states of knowledge according to the amount of information they contain. We define:

Definition 28. Let $K = \langle \langle u_1, k_1 \rangle, \ldots, \langle u_m, k_m \rangle \rangle$ and $K' = \langle \langle v_1, h_1 \rangle, \ldots, \langle v_p, h_p \rangle \rangle$ be members of $\mathscr{K}^{\Omega}$. We say that $K \leqslant K'$ (K is *more informative than* K') iff $\{u_1, \ldots, u_m\} \supseteq \{v_1, \ldots, v_p\}$ and for every $d \geqslant 0$, if $v_i = u_r < u_{r+1} < \ldots < u_{r+d+1} = v_{i+1}$, then $h_{i+1} = k_{r+1} + \ldots + k_{r+d+1}$.

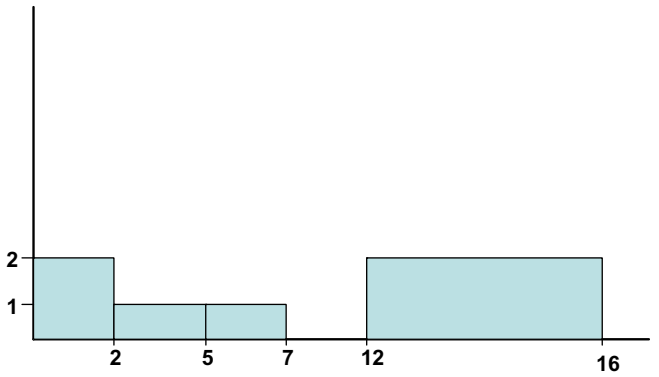


Fig. 4.1. An example of knowledge state.

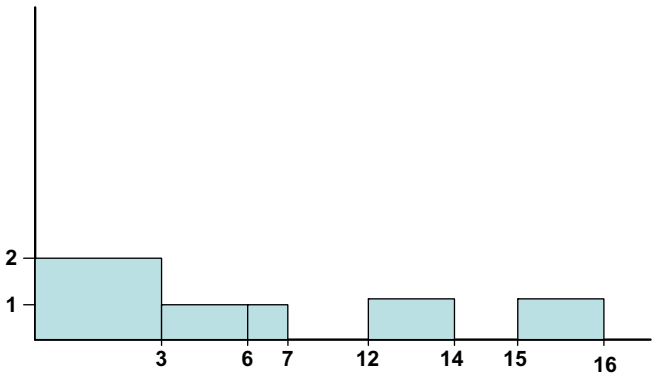


Fig. 4.2. Another example of knowledge state.

Example 29. The state K of Example 27 and the state

$$J = \langle\langle 5,3\rangle, \langle 12,1\rangle, \langle 16,2\rangle\rangle$$

are such that $K \leqslant J$.

If we restrict ourselves to states of knowledge arising from a *single* game $\Gamma = \langle \Omega, S, \mu\rangle$, with $\Omega = \{1,\ldots,N\}$ and $S = \{a_1,\ldots,a_k\}$, clearly its *solution* $0_\Gamma = \langle\langle 1,h_1\rangle,\ldots,\langle N,h_n\rangle\rangle$ - the state of knowledge whose set of cut-off points includes the whole search space - is the most informative state according to $\leqslant$, while the initial state $1_\Gamma = \langle\langle N, \sum_{i\leqslant k}\mu(a_i)\rangle\rangle$ is the least informative state according to the same relation. At this stage, we assume that any game Γ goes on until some solution state of the form $0_\Gamma = \langle\langle 1,h_1\rangle,\ldots,\langle N,h_n\rangle\rangle$ has been reached, although we will subsequently remove this rather unnatural assumption.

Next, we define a relation of *compatibility* between states of knowledge. Intuitively, two states of knowledge are compatible just in case it is not inconsistent to assume that they arise out of the same game (although they need not do so): a state K is compatible with a state K' if, whenever K features an interval wholly contained in an interval of K', the number of secrets associated with the former interval is smaller or equal than the number of secrets associated with the latter, and conversely.

Definition 30. Let $K = \langle\langle u_1,k_1\rangle,\ldots,\langle u_m,k_m\rangle\rangle$ and $K' = \langle\langle v_1,k_1\rangle,\ldots,\langle v_p,k_p\rangle\rangle$ be members of $\mathscr{K}^\Omega$. K is *compatible* with K' (in symbols, $K\psi K'$) iff, whenever $u_l \leqslant v_s < v_t \leqslant u_r$, we have that $\sum_{i=l-1}^{r} k_i \geqslant \sum_{j=s-1}^{t} h_j$, and whenever $v_s \leqslant u_l < u_r \leqslant v_t$, we have that $\sum_{i=l-1}^{r} k_i \leqslant \sum_{j=s-1}^{t} h_j$.

Example 31. The states K and K' of Example 27 are compatible states. On the other hand, K in the same example is not compatible with

$$K'' = \langle\langle 6,0\rangle, \langle 10,3\rangle, \langle 16,3\rangle\rangle.$$

Lemma 32. *ψ is a similarity relation on $\mathscr{K}^\Omega$.*

Proof. Clearly, any state K is compatible with itself, whence $\langle K, K\rangle \in \psi$. Symmetry of the relation is evident from the definition. □

We now introduce two *partial* operations on states of knowledge, which are only defined on pairs of *mutually compatible* states.

Definition 33. Let $K = \langle\langle u_1, k_1\rangle, \ldots, \langle u_m, k_m\rangle\rangle$ and $K' = \langle\langle v_1, h_1\rangle, \ldots, \langle v_p, h_p\rangle\rangle$ be members of $\mathscr{K}^{\Omega}$ s.t. $K\psi K'$. $K \wedge K'$ is the state $\langle\langle w_1, e_1\rangle, \ldots, \langle w_s, e_s\rangle\rangle$, where $\{w_1, \ldots, w_s\} = \{u_1, \ldots, u_m\} \cup \{v_1, \ldots, v_p\}$, and the e_a's are determined in such a way that:

(1) if $w_i = u_j$, then $\sum_{a=1}^{i} e_a = \sum_{b=1}^{j} k_b$, and
(2) if $w_i = v_j$, then $\sum_{a=1}^{i} e_a = \sum_{b=1}^{j} h_b$.

Definition 34. Let $K = \langle\langle u_1, k_1\rangle, \ldots, \langle u_m, k_m\rangle\rangle$ and $K' = \langle\langle v_1, h_1\rangle, \ldots, \langle v_p, h_p\rangle\rangle$ be members of $\mathscr{K}^{\Omega}$ s.t. $K\psi K'$. Let $K \wedge K'$ be the state $\langle\langle w_1, e_1\rangle, \ldots, \langle w_s, e_s\rangle\rangle$. Then, $K \to K'$ is the state $\langle\langle z_1, l_1\rangle, \ldots, \langle z_r, l_r\rangle\rangle$, where $\{z_1, \ldots, z_r\} = \{v_1, \ldots, v_p\} - \{u_1, \ldots, u_m\}$ and the l_b's are determined in such a way that

(★) if $w_j = z_i$, then $\sum_{b=1}^{j} l_b = \sum_{a=1}^{i} e_a$.

Example 35. If K, K' are the states of Example 27, $K \wedge K'$ and $K \to K'$ are depicted in Figs. 4.3 and 4.4.

If we restrict ourselves, once again, to states of knowledge arising from a single game $\Gamma = \langle\Omega, S, \mu\rangle$, the operations of meet and implication are no longer partial, but *total* operations, since all knowledge states are mutually compatible. In such a context, it makes sense to introduce a *negation* operation as follows:

$$\neg_{\Gamma} K = K \to 0_{\Gamma}$$

Once we are endowed with this operation, nothing prevents us from defining a family of *join* operations (one for each game Γ), each of which is once again defined only on pairs of compatible states, via the De Morgan law:

$$K \vee_{\Gamma} K' = \neg_{\Gamma}\left(\neg_{\Gamma} K \wedge \neg_{\Gamma} K'\right)$$

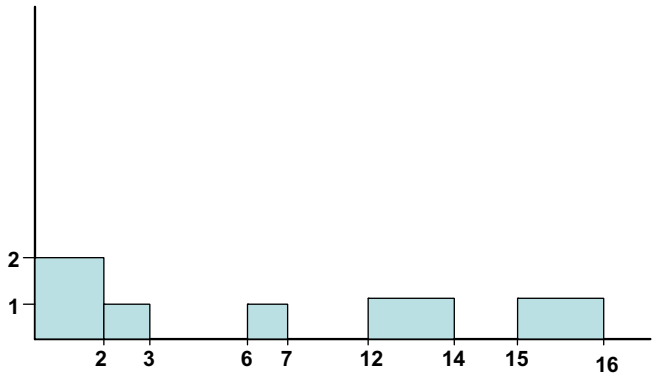


Fig. 4.3. A representation of the meet of the states in Example 2.7.

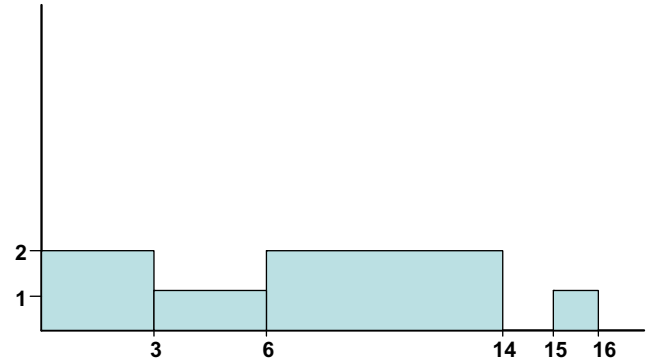


Fig. 4.4. A representation of the implication of the states in Example 2.7.

It is easy to see that (irrespective of the choice of Γ) the set of cut-off points in $K \vee_\Gamma K'$ is the *intersection* of the sets of cut-off points of K, K' (plus N, which is always a cut-off point). Now, we show that the order $\leqslant$ coincides with the order induced by the meet operation.

Lemma 36. *$K \leqslant K'$ iff $K \wedge K' = K$.*

Proof. Let $K = \langle\langle u_1, k_1\rangle, \ldots, \langle u_m, k_m\rangle\rangle$ and $K' = \langle\langle v_1, h_1\rangle, \ldots, \langle v_p, h_p\rangle\rangle$ be members of $\mathscr{K}^\Omega$ s.t. $K \leqslant K'$. By definition of $\leqslant$, $\{u_1, \ldots, u_m\} \supseteq \{v_1, \ldots, v_p\}$ and, whenever $v_x = u_r < \ldots < u_t = v_y$, $\sum_{i=r-1}^{t} k_i = \sum_{j=x-1}^{y} h_i$. Now, supposing that $v_s \leqslant u_l < u_r \leqslant v_t$, we have that $\sum_{i=l-1}^{r} k_i \leqslant \sum_{j=s-1}^{t} h_j$. Since $\{u_1, \ldots, u_m\} \supseteq \{v_1, \ldots, v_p\}$, there are two natural numbers u_x, u_y in $\{u_1, \ldots, u_m\}$ s.t. $u_x = v_s$ and $u_y = v_t$. Thus $u_x = v_s \leqslant u_l < u_r \leqslant v_t = u_y$, and then, by definition of $\leqslant$, $\sum_{i=r-1}^{t} k_i = \sum_{j=x-1}^{y} h_i$. An analogous argument holds in case $u_l \leqslant v_s < v_t \leqslant u_r$. Therefore, $K \psi K'$, which means that $K \wedge K'$ is defined. $K \wedge K'$ is the state $\langle\langle w_1, e_1\rangle, \ldots, \langle w_s, e_s\rangle\rangle$, where

$$\{w_1, \ldots, w_s\} = \{u_1, \ldots, u_m\} \cup \{v_1, \ldots, v_p\} = \{u_1, \ldots, u_m\}$$

and if $w_i = u_j$ (which is the only case to consider), then $\sum_{a=1}^{i} e_a = \sum_{b=1}^{j} k_b$. This implies $K \wedge K' = K$, which is enough for our conclusion.

Conversely, let $K \wedge K' = K$. Since $K \wedge K'$ is defined, we have that $K \psi K'$. By definition of meet, the cut-off points of $K \wedge K'$ are the cut-off points of K. Suppose $v_x = u_r \leqslant \ldots \leqslant u_t = v_y$; by compatibility $\sum_{i=r-1}^{t} k_i \leqslant \sum_{j=x-1}^{y} h_i$, and, since ψ is a symmetric relation, $\sum_{i=r-1}^{t} k_i \geqslant \sum_{j=x-1}^{y} h_i$. Therefore $\sum_{i=r-1}^{t} k_i = \sum_{j=x-1}^{y} h_i$, whence our claim follows. □

Theorem 37. *Let $\Gamma = \langle \Omega, S, \mu\rangle$ be a game, and let $\mathscr{K}^\Gamma$ be the set of all knowledge states arising from (permissible questions) on Γ. Then*

$$\mathbf{K}^\Gamma = \left\langle \mathscr{K}^\Gamma, \wedge, \vee_\Gamma, \neg_\Gamma, 0_\Gamma, 1_\Gamma \right\rangle$$

is dually isomorphic to the Boolean algebra $2^{|\Omega|-1}$.

Proof. Let $\Omega = \{1, \ldots, N\}$. Any state of knowledge in $\mathscr{K}^\Gamma$ will contain the cut-off point N. Now, consider the mapping

$$f : \mathbf{2}^{N-1} \to \mathbf{K}^\Gamma$$

given by $f(\{x_1, \ldots, x_k\}) = \langle\langle x_1, h_1\rangle, \ldots, \langle x_k, h_k\rangle, \langle N, h_{k+1}\rangle\rangle$. This is the required (dual) isomorphism, since two states of knowledge on Γ count as distinct if and only if they have different cut-off points. □

As we remarked above, the assumption according to which any game Γ goes on until a knowledge state has been reached where each interval is a singleton is rather awkward from a game-theoretical point of view. Intuitively, it would look as though a game should stop when Bob's knowledge state is such that the only intervals which are not singletons are intervals containing no secrets. If, for example, $\Omega = \{1, 2, 3, 4\}$, $S = \{4\}$ and $\mu(4) = 1$, the state $\langle\langle 3, 0\rangle, \langle 4, 1\rangle\rangle$ can be considered as a solution to all intents and purposes, even if its set of cut-off points does not coincide with the whole search space. In other words, one should do away with some irrelevant distinctions, identifying with one another states which may be plausibly taken as representing the same information. In particular, we should consider as equivalent any two states of knowledge which differ at most for a different subdivision of intervals containing no secrets.

Formally, we proceed as follows:

Definition 38. A knowledge state $K = \langle\langle u_1, k_1\rangle, \ldots, \langle u_m, k_m\rangle\rangle$ is said to be *in normal form* iff for $i = 1, \ldots, m-1$, if $k_i = 0$, then $k_{i+1} > 0$.

Intuitively, a state of knowledge is in normal form whenever any two consecutive intervals with no secrets have been lumped together. Consequently, given any state K, we obtain a state $N(K)$ in normal form – called the *normal form* of K - by iterating the following operation: for $i = 1, \ldots, m-1$, if $k_i = k_{i+1} = 0$, then delete $\langle u_i, k_i\rangle$ from K.

Definition 39. The state K is equivalent to K' (in symbols: $K \theta K'$), if they have the same normal form, i.e. if $N(K) = N(K')$.

Example 40. The state K of Example 27 is equivalent to the state $K'' = \langle\langle 2, 2\rangle, \langle 5, 1\rangle, \langle 7, 1\rangle, \langle 10, 0\rangle, \langle 12, 0\rangle, \langle 16, 2\rangle\rangle$.

We easily obtain the following result, which we state without a proof:

Lemma 41. *θ is an equivalence relation on $\mathscr{K}^\Omega$.*

As a consequence, the quotient $\mathscr{K}^\Omega/\theta$ can be identified with the set of all normal states. If we revert to the Boolean algebra $\mathbf{K}^\Gamma$ of all knowledge states arising from a single game, it makes sense to inquire whether the subset $N(\mathscr{K}^\Gamma)$ of all normal states in $\mathscr{K}^\Gamma$ is the universe of a subalgebra of $\mathbf{K}^\Gamma$. Unfortunately this is not the case, in general. However, we have the following:

Lemma 42. *Let $\mathbf{K}^\Gamma = \langle \mathscr{K}^\Gamma, \wedge, \vee_\Gamma, \neg_\Gamma, 0_\Gamma, 1_\Gamma\rangle$ be the Boolean algebra of all knowledge states arising from (permissible questions) on Γ. Furthermore, let $\mathbf{N}(\mathbf{K}^\Gamma) = \langle N(\mathscr{K}^\Gamma), \wedge', \vee'_\Gamma, \neg'_\Gamma, 0'_\Gamma, 1'_\Gamma\rangle$, where for any operation symbol f,*

$$f'(K_1,\ldots,K_n) = N(f(K_1,\ldots,K_n)).$$

Then: i) $\mathbf{N}(\mathbf{K}^{\Gamma})$ *is a pseudocomplemented lattice; ii)* $\langle N(\mathscr{K}^{\Gamma}), \vee'_{\Gamma}, 1'_{\Gamma}\rangle$ *is a join subsemilattice with unit of the corresponding reduct of* $\mathbf{K}^{\Gamma}$.

Proof

(i) Since $N(\mathscr{K}^{\Gamma})$ is a finite set, if we can show that $\langle N(\mathscr{K}^{\Gamma}), \wedge', 1'_{\Gamma}\rangle$ is a semilattice with maximum we are automatically guaranteed that

$$\langle N(\mathscr{K}^{\Gamma}), \wedge', \vee'_{\Gamma}, 0'_{\Gamma}, 1'_{\Gamma}\rangle$$

is a bounded lattice. Now, given two normal states K,J, we put $K \leqslant' J$ whenever there are states K^*,J^* s.t. $K^* \leqslant J^*$, $K\theta K^*$ and $J\theta J^*$. One can easily see from Definitions 28, 39 that $\leqslant'$ is a partial order on $N(\mathscr{K}^{\Gamma})$ and that $1'_{\Gamma} = 1_{\Gamma}$ is its maximum. What remains to show is that $K\wedge' J \leqslant' K,J$ and that if $L \leqslant' K,J$ then $L \leqslant' K\wedge' J$. As regards the latter item, since L,K,J are supposed to be normal states, what we must prove is that $L \leqslant K,J$ implies $L \leqslant N(K\wedge J)$; however, by Lemma 36 $L \leqslant K,J$ implies $L \leqslant K\wedge J$, whence our conclusion follows since $K\wedge J \leqslant N(K\wedge J)$. As regards the former, once again by Lemma 36, $N(K\wedge J)$ is θ-equivalent to $K\wedge J$ and $K\wedge J \leqslant K,J$ – i.e. $K\wedge' J \leqslant' K,J$. So we get a lattice and it can be checked that the join of such a lattice coincides with $\vee'_{\Gamma}$. Finally, we must establish that $\neg'_{\Gamma}K$ is the pseudocomplement of K. As a first step, we show that $N(K\wedge\neg'_{\Gamma}K) = N(0_{\Gamma})$. Given a state

$$M = \langle\langle u_1,k_1\rangle,\ldots,\langle u_m,k_m\rangle\rangle,$$

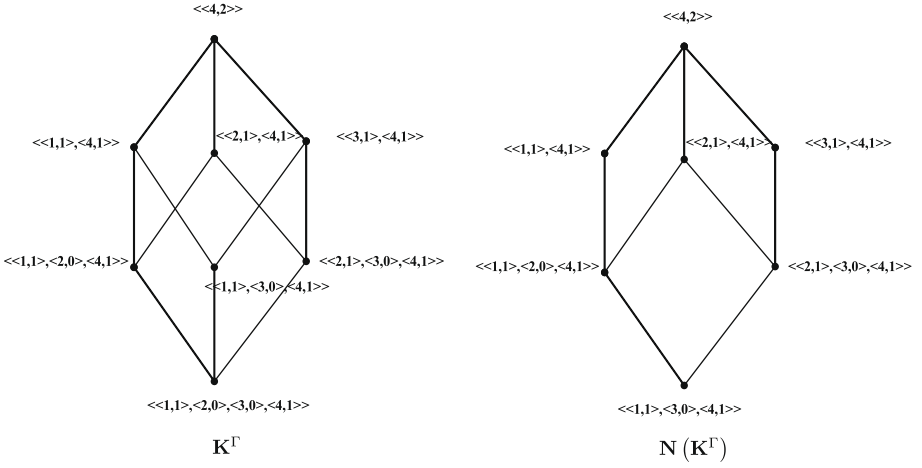
we call $\langle u_i,k_i\rangle$ M – *unavoidable* just in case either (i) $k_i \neq 0$ or (ii) $k_i = 0$ but $k_{i+1} \neq 0$. Now, the set of cut-off points of $K\wedge\neg'_{\Gamma}K$ comprises the whole search space minus any cut-off point which is not $\neg_{\Gamma}K$-unavoidable. This means that all the 0_{Γ}-unavoidable cut-off points are there, whence by normalising $K\wedge\neg'_{\Gamma}K$ we get exactly to $N(0_{\Gamma})$. The second step amounts to showing that $N(K\wedge J) = N(0_{\Gamma})$ implies $J \leqslant \neg'_{\Gamma}K$ (since $J,\neg'_{\Gamma}K$ are normal). If $N(K\wedge J) = N(0_{\Gamma})$, then $K\wedge J$ must contain all 0_{Γ}-unavoidable cut-off points. If all such points are already in J, we have our conclusion. If u_i is a 0_{Γ} -unavoidable cut-off point of $K\wedge J$ which is not in J, it will be in K and consequently not in $\neg'_{\Gamma}K$. Once again, therefore, we conclude that $J \leqslant \neg'_{\Gamma}K$.

(ii) Since the initial state $1'_{\Gamma}$ is obviously normal whenever there is at least one secret, we must prove that, given any two states $L = \langle\langle x_1,l_1\rangle,\langle x_2,l_2\rangle,\ldots,\langle x_r,l_r\rangle\rangle, K = \langle\langle y_1,k_1\rangle,\langle y_2,k_2\rangle,\ldots,\langle y_s,k_s\rangle\rangle$ in $N(\mathscr{K}^{\Gamma})$, $L\vee' K = L\vee K$. Let

$$L\vee K = \langle\langle z_1,h_1\rangle,\langle z_2,h_2\rangle,\ldots,\langle z_m,h_m\rangle\rangle,$$

and suppose ex absurdo that for some $i \leqslant m$, $h_i = h_{i+1} = 0$. Then there are natural numbers j_1,j_2,p_1,p_2 s.t. $z_i = x_{j_1} = y_{j_2}$ and $z_{i+1} = x_{j_1+p_1} = y_{j_2+p_2}$. Moreover, $l_{j_1} \neq 0$ or $l_{j_1+p_1} \neq 0$; likewise, $k_{j_2} \neq 0$ or $k_{j_2+p_2} \neq 0$; but this is a contradiction with the fact that $L,K \leqslant L\vee K$. □

Example 43. Let $\Gamma = \langle\Omega,S,\mu\rangle$, with $\Omega = \{1,2,3,4\}$, $S = \{1,4\}$ and $\mu(1) = \mu(4) = 1$. The Hasse diagrams of $\mathbf{K}^{\Gamma}$ and $\mathbf{N}(\mathbf{K}^{\Gamma})$ are reproduced below.



$\mathbf{K}^{\Gamma}$ $\quad\quad$ $\mathbf{N}(\mathbf{K}^{\Gamma})$

Notice that $\mathbf{N}(\mathbf{K}^{\Gamma})$ is a pseudocomplemented nondistributive lattice (it has an isomorphic copy of $\mathbf{N}_5$ as a sublattice). Also observe that all the joins of $\mathbf{N}(\mathbf{K}^{\Gamma})$ are preserved, while some meets are not preserved. For example,

$$\langle\langle 1,1\rangle,\langle 2,0\rangle,\langle 4,1\rangle\rangle \wedge \langle\langle 2,1\rangle,\langle 3,0\rangle,\langle 4,1\rangle\rangle = \langle\langle 1,1\rangle,\langle 2,0\rangle,\langle 3,0\rangle,\langle 4,1\rangle\rangle$$

and $\langle\langle 1,1\rangle,\langle 2,0\rangle,\langle 3,0\rangle,\langle 4,1\rangle\rangle$ is not a normal state. We have instead

$$\langle\langle 1,1\rangle,\langle 2,0\rangle,\langle 4,1\rangle\rangle \wedge' \langle\langle 2,1\rangle,\langle 3,0\rangle,\langle 4,1\rangle\rangle = \langle\langle 1,1\rangle,\langle 3,0\rangle,\langle 4,1\rangle\rangle$$

Finally, we characterise those games Γ such that $\mathbf{N}(\mathbf{K}^{\Gamma})$ is, respectively, a *chain* and a *Boolean algebra* in terms of properties of their multisets of secrets.

Lemma 44. *The following are equivalent:*

1. $\Gamma = \langle \Omega, S, \mu\rangle$ *is such that* $S = \{a_1\}$ *and either* $a_1 = 1$ *or* $a_1 = N$;
2. $\mathbf{N}(\mathbf{K}^{\Gamma})$ *is a pseudocomplemented chain.*

Proof. $\Rightarrow$ Let a_1 be the unique secret of S and let $a_1 = 1$ or $a_1 = N$. W.l.g., let $a_1 = 1$. Therefore there exists a unique state $K = \langle\langle N-1,1\rangle,\langle N,0\rangle\rangle$ which is a subcover of $1_{\Gamma} = \langle\langle N,1\rangle\rangle$. Again, using the same argument K has the state $K' = \langle\langle N-2,1\rangle,\langle N,0\rangle\rangle$ as its unique subcover. Iterating this process we obtain that $\mathbf{N}(\mathbf{K}^{\Gamma})$ is a chain.

$\Leftarrow$ (a) Suppose S contains more than one secret. W.l.g. let us assume $S = \{a_1, a_2\}$ and that the cardinality of $N(\mathscr{K}^{\Gamma})$ is even (the argument can be straightforwardly adapted to the case of odd cardinality). If a_1, a_2 are different from 1 and N consider the states $K = \langle\langle 1,0\rangle,\langle N,2\rangle\rangle$ and $K' = \langle\langle N-1,2\rangle,\langle N,0\rangle\rangle$; clearly $K \not\leqslant K'$ and $K' \not\leqslant K$. If $a_1 = 1$ and $a_2 \neq N$ consider the states $K = \langle\langle N-1,2\rangle,\langle N,0\rangle\rangle$ and $K' = \langle\langle 1,1\rangle,\langle N,1\rangle\rangle$; again $K \not\leqslant K'$ and $K' \not\leqslant K$. If $a_1 \neq 1$ and $a_2 = N$ an analogous argument applies. If $a_1 = 1$ and $a_2 = N$ there exist two states $K = \langle\langle \frac{N}{2},1\rangle,\langle \frac{N}{2}+1,1\rangle\rangle$ and $K' = \langle\langle \frac{N}{2}-1,1\rangle,\langle \frac{N}{2},1\rangle\rangle$ such that $K \not\leqslant K'$ and $K' \not\leqslant K$.

(b) Suppose now that S contains just one secret a_1, but that a_1 is different from 1 and N. It can be seen that there are states $K = \langle\langle a_1,1\rangle,\langle N,0\rangle\rangle$ and $K' = \langle\langle a_1-1,0\rangle,\langle N,1\rangle\rangle$ s.t. $K \not\leqslant K'$ and $K' \not\leqslant K$. $\square$

Lemma 45. *The following are equivalent:*

1. $\Gamma = \langle \Omega, S, \mu\rangle$ *is such that if* $m, m+1 \in \Omega$, *then either* $m \in S$ *or* $m+1 \in S$;
2. $\neg'_{\Gamma}$ *is involutive.*
3. $\mathbf{N}(\mathbf{K}^{\Gamma})$ *is a Boolean algebra.*

Proof. $2 \Rightarrow 1$. Let $0'_{\Gamma} = \langle\langle w_1,h_1\rangle,\ldots,\langle w_m,h_m\rangle\rangle$ and $K = \langle\langle u_1,k_1\rangle,\ldots,\langle u_n,k_n\rangle\rangle$. By definition $\neg'_{\Gamma}$ is involutive iff, for any state K: $\neg'_{\Gamma}\neg'_{\Gamma}K = K$, i.e. $(K \to 0'_{\Gamma}) \to 0'_{\Gamma} = K$. But from the definition of $\to$ and an elementary calculation, if this last condition holds, then $\{w_1,\ldots,w_m\} - (\{w_1,\ldots,w_m\} - \{u_1,\ldots,u_n\}) = \{u_1,\ldots y,u_n\}$, whence 0_{Γ} is normal and thus condition 1. is satisfied.

$3 \Rightarrow 2$. Trivial.

$1 \Rightarrow 3$. Suppose that if $m, m+1 \in \Omega$, then either $m \in S$ or $m+1 \in S$. This implies that all the states are normal and therefore $\mathbf{N}(\mathbf{K}^{\Gamma}) = \mathbf{K}^{\Gamma}$, whence our conclusion follows from Theorem 37. $\square$

5. Conclusions

Let us now briefly recap what we have achieved in this paper. In Section 2 we introduced a cooperative variant of the Guessing Secrets problem in which the information in the possession of the respondent is incomplete, showing that the number of questions to be asked in order to reconstruct the probability assignment involved therein is bounded above by a polynomial function whose arguments are the cardinality of the search space and the number of secrets. In Section 3 we modified the rules of such a game, allowing the respondent to *lie* a certain number of times and obtaining in this way a common generalisation of the GSP and of *Ulam game*. Finally, in Section 4 we focused on two algebraic structures relevant to the cooperative GSP: i) the algebra of all states of knowledge induced by games on a fixed search space; ii) the algebra $\mathbf{N}(\mathbf{K}^{\Gamma})$ of states of knowledge arising from a single designated game Γ. Our main result, here, was that $\mathbf{N}(\mathbf{K}^{\Gamma})$ is a pseudocomplemented lattice whose join semilattice reduct is embeddable into the corresponding reduct of the Boolean algebra $\mathbf{2}^{N-1}$, where N is the cardinality of the search space.

Some problems concerning the relationships between the structure of a game Γ and the algebraic properties of $\mathbf{N}(\mathbf{K}^{\Gamma})$ remain open. In particular, we draw the interested reader's attention to the following one:

Problem 46. Give necessary and sufficient conditions for $\mathbf{N}(\mathbf{K}^{\Gamma})$ to be distributive.

References

[1] N. Alon, V. Guruswam, T. Kaufman, M. Sudan, Guessing secrets efficiently via list decoding, ACM Transactions on Algorithms 3 (4) (2007) 1–16.
[2] R. Ahlswedea, F. Cicalese, C. Deppe, Searching with lies under error cost constraints, Discrete Applied Mathematics 156 (2008) 1444–1460.
[3] L. Chung, R. Graham, F.T. Leighton, Guessing secrets, Electronic Journal of Combinatorics 8 (2001).

[4] L. Chung, R. Graham, L. Lu, Guessing secrets with inner product questions, in: Proceedings of SODA-02, ACM, 2002, pp. 247–253.
[5] R. Cignoli, I.M.L. D'Ottaviano, D. Mundici, Algebraic Foundations of Many-Valued Reasoning, Kluwer, Dordrecht, 1999.
[6] J. Czyzowicz, D. Mundici, A. Pelc, Ulam's searching game with lies, Journal of Combinatorial Theory, Series A 52 (1989) 62–76.
[7] A. Del Lungo, G. Louchard, C. Marini, F. Montagna, The Guessing Secrets problem: a probabilistic approach, Journal of Algorithms 55 (2005) 142–176.
[8] R. Diestel, Graph Theory, Springer, Berlin, 2000.
[9] M. Fernandez, M. Soriano, Efficient recovery of secrets, in: Proceedings of ITCC-04, ACM, 2004, vol. 4, p. 763.
[10] M. Fernandez, M. Soriano, J. Lotrina, Tracing traitors by guessing secrets: the q-ary case, in: B.H. Deng, F. Bao, H. Pang, J. Zhou (Eds.), Information Security Practice and Experience, Springer, Berlin, 2005, pp. 61–73.
[11] C. Marini, F. Montagna, Probabilistic variants of Ulam's game and many valued logic, Task Quarterly 9 (3) (2005) 317–335.
[12] A. Martin del Rey, G. Rodriguez Sanchez, Selling multiple secrets to a single buyer, Information Sciences 179 (11) (2009) 1657–1662.
[13] D. Mundici, The logic of Ulam's game with lies, in: C. Bicchieri, M.L. Dalla Chiara (Eds.), Knowledge, Belief and Strategic Interaction, Cambridge University Press, Cambridge, 1992, pp. 275–284.
[14] M. Nathanson, Quantum guessing via Deutsch-Jozsa, arXiv:quant-ph/0301025v2.
[15] I. Reay, S. Dick, J. Miller, An analysis of privacy signals on the World Wide Web: past, present and future, Information Sciences 179 (8) (2009) 1102–1115.
[16] A. Pelc, Solution of Ulam's problem on searching with a lie, Journal of Combinatorial Theory, Series A 44 (1987) 129–140.
[17] J. Spencer, Ulam's searching game with a fixed number of lies, Theoretical Computer Science 95 (1992) 307–321.
[18] C. Wang, W. Tang, R. Zhao, Static Bayesian games with finite fuzzy types and the existence of equilibrium, Information Sciences 178 (2008) 4688–4698.