Feedback coding and many-valued logic

Abstract

DANIELE MUNDICI*

The basic problem of feedback coding is presented by Rényi [9, page 47] as follows:

> [...] I made up the following version, which I called "Bar-kochba with lies". Assume that the number of questions which can be asked to figure out the "something" being thought of is fixed and the one who answers is allowed to lie a certain number of times. The questioner, of course, doesn't know which answer is true and which is not. Moreover the one answering is not required to lie as many times as is allowed. For example, when only two things can be thought of and only one lie is allowed, then 3 questions are needed [...] If there are four things to choose from and one lie is allowed, then five questions are needed. If two or more lies are allowed, then the calculation of the minimum number of questions is quite complicated [...] It does seem to be a very profound problem [...]

The same problem is posed by Ulam in [10, page 281], as the problem of guessing an unknown m-bit number by asking a minimum of yes-no questions, in a game of Twenty Questions with up to e lies in the answers.

Here two players called Carole and Paul fix a finite space S with $|S|$ elements. Then Carole chooses an element $x_{secret} \in S$ and Paul must find it by asking a minimum of yes-no questions, with the stipulation that up to e of Carole's answers may be erroneous/mendacious/inaccurate. From Paul's viewpoint it is indifferent whether wrong answers arise because Carole is unable/unwilling to answer correctly, or else Carole is always sincere but distortion may corrupt up to e of her yes-no answers. Under this latter hypothesis, *Ulam–Rényi games belong to Berlekamp's communication theory with feedback* [1].

In the particular case when all questions are asked non-adaptively, Paul's strategies are the same as e-error-correcting codes.

*Department of Mathematics "Ulisse Dini", University of Florence, Viale Morgagni 67/A, 50134 Florence, Italy. e-mail: `mundici@math.unifi.it`

One easily sees that no solution to the problem exists using less than $N_{\min}(|S|, e)$ bits, where the *sphere-packing bound* $N_{\min}(|S|, e)$ is the smallest integer $q \geq 0$ satisfying the classical inequality $2^q \geq |S| \sum_{j=0}^{e} \binom{q}{j}$. Let us agree to say that the secret number can be guessed by a *perfect* strategy iff the number of questions coincides with the smallest integer $q \geq 0$ satisfying the above inequality.

The following result is well known to researchers in error-correcting codes:

Fact 0: Non-existence of perfect error-correcting codes
If no feedback is allowed, a perfect strategy does not exist in general, already in case of 2 *errors.*

By contrast, the following result is the output of extensive research during the last two decades (see the survey papers [8, 4] and references therein):

Fact 1: Existence of perfect error-correcting codes with feedback
If feedback is allowed then for every number e of errors, a number can be guessed in general, using a perfect strategy.

It turns out [2, 4, 5] that perfect error-correcting codes also exist under very weak conditions on feedback:

Fact 2: Minimum feedback is sufficient for perfect coding
Paul can always find x_{secret} using a perfect strategy where feedback occurs only once: Paul asks a first batch of nonadaptive questions, and then, only depending on the answers to these questions, he asks a second batch of non-adaptive questions.

In the light of the negative Fact 0, the above result states that perfect error-correcting coding only requires *minimum* (nonzero) feedback.

* * * * * * *

Enter many-valued logic. A natural generalization of Rényi-Ulam games is obtained by assuming that increasingly noisy channels $1, 2, \ldots, m$ are available to Carole for her answers to Paul. Naturally enough, for any $i < j$, the information sent on channel i supersedes the cheaper information given on j. Precisely as in the Rényi-Ulam game, [7] Paul's state of knowledge during a multichannel game is uniquely determined by Carole's answers. Since two equal answers to the same repeated question are more informative than a single answer, Carole's answers are recorded by Paul as a *multiset*. The family K of Paul's states of knowledge has an interesting structure: first of all, K comes equipped with a partial order $s \leq t$ (read: " state s is more restrictive than t"). Further, K is endowed with a conjunction operation $\odot$ canonically arising from multiset union. The initial state 1 (the empty multiset) is neutral for $\odot$. Finally, K is equipped with an operation $\rightarrow$ given by the residual of $\odot$ with respect to the partial order of K.

Generalizing the interpretation [7] of one-channel games in Łukasiewicz infinite-valued logic, it will be shown that Paul's states of knowledge in multichannel games are governed by (and provide a natural semantics to) Hájek's basic propositional logic BL, [6]. Proofs are given elsewhere [3].

References

[1] E. R. BERLEKAMP, Block coding for the binary symmetric channel with noiseless, delayless feedback. In: *Error-correcting Codes.* (Mann, H. B., Ed.) Wiley, New York, (1968), p. 330-335.

[2] F. CICALESE, D. MUNDICI, Perfect two fault-tolerant search with minimum adaptiveness, *Advances in Applied Mathematics*, 25:65-101, 2000.

[3] F. CICALESE, D. MUNDICI, Recent developments of feedback coding, and its relations with many-valued logic. *Manuscript*, 2005.

[4] F. CICALESE, D. MUNDICI, U. VACCARO, Rota-Metropolis cubic logic and Ulam-Rényi games, In: *Algebraic Combinatorics and Computer Science: a tribute to Gian-Carlo Rota*, (H. Crapo, D. Senato, Eds.), Springer-Verlag, Milan, (2001), pp. 197–244.

[5] F. CICALESE, D. MUNDICI, U. VACCARO, Least adaptive optimal search with unreliable tests. *Theoretical Computer Science*, 270:877-893, 2002.

[6] P. HÁJEK, *Metamathematics of fuzzy logic.* Kluwer, Dordrecht. 1998. (*Trends in Logic, Studia Logica Library*)

[7] D. MUNDICI, The logic of Ulam's game with lies, In: Knowledge, Belief and Strategic Interaction, *Cambridge Studies in Probability, Induction, and Decision Theory*, (1992), pp. 275-284.

[8] A. PELC, Searching games with errors: fifty years of coping with liars, *Theoretical Computer Science,* 270: 71-109, 2002.

[9] A. RÉNYI, *Napló az információelméletről*, Gondolat, Budapest, 1976. (English translation: *A Diary on Information Theory*, J.Wiley and Sons, New York, 1984).

[10] S. ULAM, *Adventures of a Mathematician*, Scribner's, New York, 1976.