DOI: 10.2507/37th.daaam.proceedings.xxx

A MISSION-BASED COLLABORATIVE LEARNING GAME FOR INFORMATION THEORY

Silvio Papic, Edijan Secic and Toma Susa

Working Paper of 37th DAAAM Symposium

Abstract

Information theory is often introduced through abstract measures and then through isolated coding and cryptographic algorithms. This can leave students able to reproduce calculations without understanding which communication constraint—limited message length, transmission noise or interception—makes a specific method necessary. The issue remains important in AI-rich learning environments, where a correct procedure or result can be obtained without establishing such functional understanding.This paper presents the design and pilot implementation of a physical mission-based collaborative learning game for applied information theory. Rather than adding competition to conventional exercises, the design makes communication procedures conditions for coordinated action. Physically separated headquarters and fleet roles exchange route commands through a channel observable to an opposing team. Mission conditions require efficient representation, error recovery and, where necessary, confidentiality; selected hand-calculable instances of source coding, error-control coding, key exchange and encryption operationalise these functions. A pilot implementation involved nineteen students from five countries and concluded with an individual integrated examination. Scores ranged from 0 to 100 points (M = 73.3, Md = 88). The pilot demonstrates the feasibility of implementing the design and assessing individual post-module performance; it identifies heterogeneous domain-level results and cases in which low domain-specific self-reported familiarity was followed by high individual performance. It does not estimate learning gain or establish comparative effectiveness.

Keywords: Information theory; serious games; game-based learning; noisy-channel communication.

1. Introduction

Information theory provides a broader framework for analysing representation, uncertainty, compression, transmission and noise; it is not defined by a particular set of algorithms. This paper focuses on selected algorithms through which these ideas can be made operational in an introductory learning setting. Shannon's communication model provides a common frame for considering source representation, channel transmission and message recovery [1]. Within this scope, Huffman coding constructs minimum-redundancy prefix-free codes [2], while arithmetic coding is a lossless source-coding method that represents a message sequence as an interval determined by a probability model, enabling compression close to the limit implied by that model [3]. Channel coding introduces structured redundancy that enables the receiver to detect and, within the capability of the code, correct transmission errors. Hamming codes provide a standard example of single-bit error correction [4]. Reed-Solomon codes are polynomial codes over finite fields that can correct multiple erroneous symbols per codeword, subject to their parameters and decoding conditions [5]. Cryptographic mechanisms address a different requirement: preventing an unintended party from reading the message. Diffie-Hellman key exchange enables communicating parties to establish a shared secret without transmitting that secret directly [6].

These algorithms are often taught as separate calculations. The resulting pedagogical problem is not only procedural execution, but recognising which communication requirement—efficient representation, reliable transmission or confidentiality—calls for which mechanism in a real communication situation, and how these mechanisms can be combined. Game-based learning may situate such procedures in goals, constraints and consequences. It should be distinguished from gamification, which may add game-design elements to an otherwise unchanged activity [7]. Game-based approaches have also been used in technical programming instruction [8]. Their educational value, however, depends on the learning activity and assessment design [9], [10], rather than following automatically from the presence of a game [11].

The paper documents the design and reports its pilot implementation in a five-day international module. The paper asks: (1) how the design connects information-theory functions within one operational scenario; (2) what patterns of individual performance appear in the integrated final examination; and (3) how students' self-reported domain-specific familiarity with selected concepts contextualises subsequent individual examination performance.

2. Design of the mission-based learning game

This mission-based collaborative learning game was conceived, designed and developed specifically for a five-day Erasmus+ Blended Intensive Programme module on information theory and secure communication. It turns communication constraints into conditions for action: teams cannot move their fleet until the required command has been prepared, transmitted and correctly interpreted. Depending on the mission phase, this requires binary encoding, source coding, error protection and/or encryption. Each team receives a route to a destination that must remain unknown to the opposing team. Movement commands were represented in a seven-bit format. The first four bits encoded the permitted cardinal-direction components in the order N, E, S and W; diagonal movement activated two direction bits. The final three bits represented the movement distance using binary weights 4, 2 and 1. For example, the command NE3 was represented as 1100 011: the prefix 1100 denotes north-east movement and the suffix 011 denotes a distance of three tiles. The seven-bit command format was chosen so that each movement instruction could serve directly as the seven information bits of a Hamming (11,7) code. Four parity bits were then added to form an eleven-bit protected transmission, allowing the receiving fleet to identify and correct a single-bit error introduced by the Game Master. A route consists of ten movement commands, expressed in a compact directional form, for example **NE7** (move seven tiles north-east) or **SE2** (move two tiles south-east). The shared communication medium is intentionally observable to both teams. Opponents may inspect intercepted commands and attempt to reconstruct the route and destination. Competitive success therefore depends both on completing one's own route and on identifying the opponent's destination before one's own is revealed.

The method applied to each message was specified by the mission conditions. Responsibility for encoding and decoding rotated among team members in successive rounds, so mission completion required distributed procedural competence rather than reliance on a single expert. Each mission route was organized as a progressively constrained sequence of movement commands. The initial commands were transmitted in clear text so that students could establish the shared command representation, coordinate headquarters and fleet roles, and observe the operational consequence of an accurately interpreted route instruction.

Subsequent commands introduced controlled transmission noise. In the Hamming phase, commands were binary encoded and protected using the Hamming code. After a team had prepared a message for transmission, the Game Master introduced one random bit error before forwarding it to the receiving fleet. The fleet had to identify and correct the error before executing the movement. Later commands required arithmetic coding as the source-representation method. Where

Working Paper of 37th DAAAM Symposium

a transmission error was imposed, source coding alone was insufficient: students also had to apply the error-control procedure required by that mission phase before the command could be recovered.

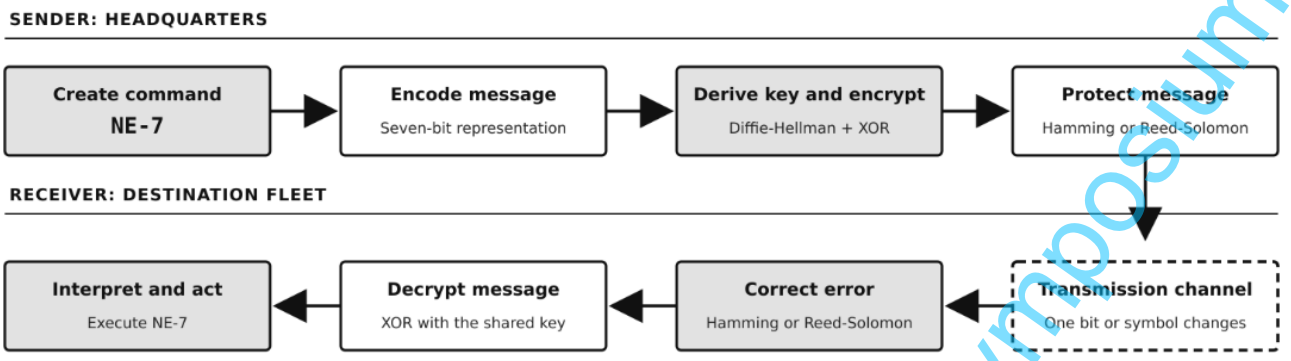

Fig. 1. Example of communication between sender and receiver

In the simplified Reed-Solomon phase, a movement command was first divided into a direction component and a distance component. Their binary representations were interpreted as two numerical finite-field symbols. In this representation, the direction binary code 1010 corresponds to the symbol 12 and the distance binary code 111 corresponds to the symbol 7. These two symbols formed the information-bearing coefficients of a first-degree message polynomial.

Redundancy was created by evaluating the message polynomial at additional agreed field elements. The mission condition specified the number of symbol errors to be corrected. The total number of transmitted symbols was determined by $n = k + 2t$, where k is the number of information symbols and t is the number of correctable symbol errors. In this implementation, the direction and distance formed two information symbols ($k = 2$). A mission requiring correction of one altered symbol used a four-symbol codeword, whereas a mission requiring correction of two altered symbols used a six-symbol codeword. Before forwarding the codeword to the receiving fleet, the Game Master deliberately changed the number of transmitted symbols specified by the mission. The receiving team had to use the redundant information to locate and correct the altered symbols, reconstruct the message polynomial and recover the original direction and distance values before executing the movement command.

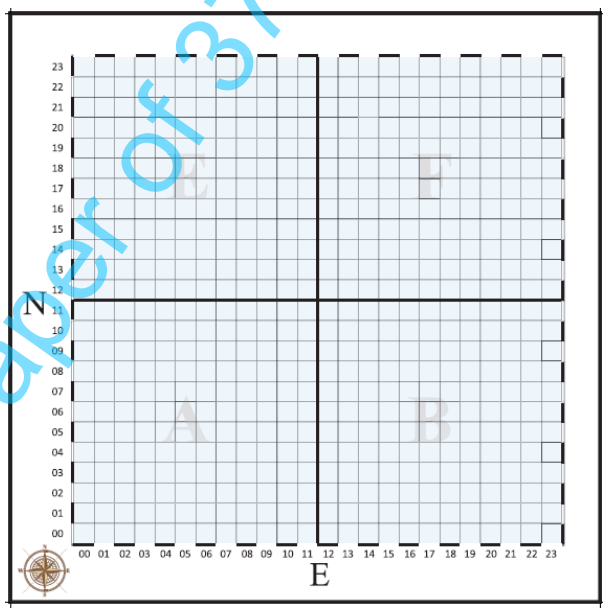

Fig. 2. Design of the 24 × 24 game board

The final mission phase combined reliability and confidentiality. The headquarters and fleet first established a shared value through Diffie-Hellman key exchange. This value was then used as the key for XOR encryption of the command. The encrypted bit sequence was subsequently protected using the error-control procedure required by the mission before transmission over the observable channel. Diffie-Hellman enabled the two roles to derive the shared value required for encryption without transmitting that value directly. The Game Master introduced the prescribed transmission disturbance

Working Paper of 37th DAAAM Symposium

before forwarding the message to the receiving fleet. The fleet had to apply the required error-recovery procedure to the received transmission, decrypt the recovered message, and interpret the movement instruction before acting. The sequence made the dependency between communication functions explicit: source coding addressed representation efficiency, Hamming and Reed-Solomon procedures addressed recovery from imposed transmission disturbances, and Diffie-Hellman exchange with XOR encryption addressed confidentiality on a channel observable to the opposing team.

2.1. Physical game environment and roles

The implementation of the game uses five separate 24 × 24 boards. Each competing team has a headquarters board and a fleet board, while the Game Master maintains a fifth board containing the reference mission routes and the information required to verify commands and game-state changes. Headquarters, fleet personnel and the opposing team are physically separated so that they cannot inspect one another's boards directly.

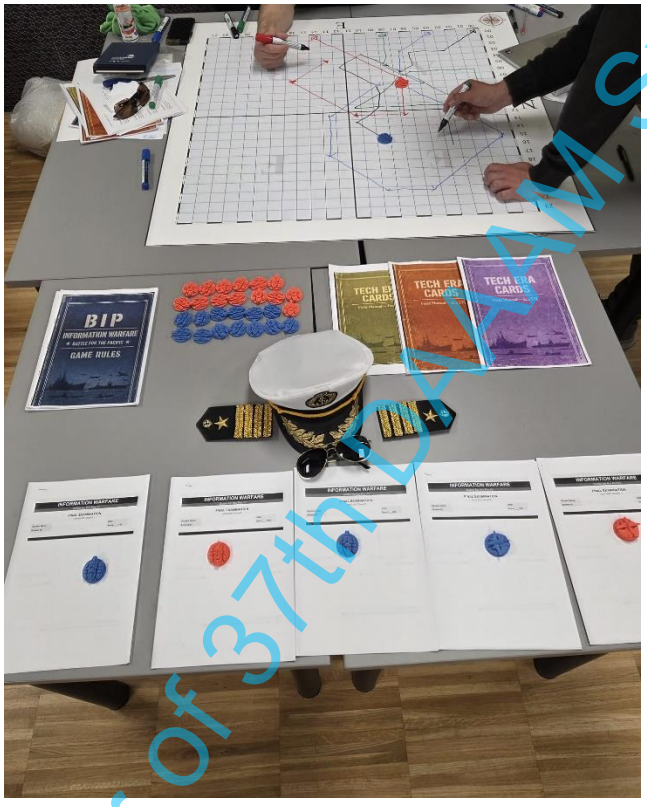

Fig. 3. Board and game in use and learning materials

This arrangement makes communication operationally necessary. A headquarters must transmit each command to its fleet before the fleet can act, while the Game Master verifies whether the decoded command corresponds to the assigned route. Physical separation prevents teams from obtaining route information through direct visual observation rather than through the communication channel.

All transmitted messages are observable on the shared channel. Each team must therefore communicate accurately for its own fleet to complete the assigned route before the opposing fleet. At the same time, teams attempt to decode as many intercepted opposing messages as possible. The Game Master controls the channel and introduces mission-specified disturbances, including bit errors in the Hamming phase and symbol errors in the simplified Reed-Solomon phase. Students use mission sheets, calculation sheets, coding masks and era cards to externalise intermediate representations such as codebooks, intervals, bit sequences, finite-field symbols and correction procedures. For each successive command, team members rotated between the headquarters and fleet roles. No participant could therefore remain responsible for only one procedure: successful team performance required every member to be able to apply the full set of communication procedures. This rotation created an incentive for peer explanation and mutual support, because a team's subsequent performance depended on the competence of all its members.

Working Paper of 37th DAAAM Symposium

2.2. *Scenario-driven learning progression and final mission structure*

The learning progression was designed specifically for this game. Rather than presenting algorithms in a fixed abstract sequence, the Game Master introduced new operational requirements that made the limitations of the currently available procedures visible. Students then learned and applied the mechanism required to address the newly introduced communication problem. The stages were labelled as *eras* in the game materials; this term denotes internally designed phases of the learning scenario. Initial activities established a common representation of movement commands and their binary form. Constraints on message length then created a need for efficient representation and introduced entropy, Huffman coding and arithmetic coding. The Game Master subsequently introduced transmission disturbances, making it necessary to detect or correct altered messages through parity checks, Hamming protection and the simplified Reed-Solomon procedure. Finally, the fact that all teams could observe the same communication channel created a confidentiality requirement. Students addressed this requirement by establishing a shared value through Diffie-Hellman key exchange and using it for XOR encryption. Each new requirement was therefore introduced before the corresponding procedure was taught. Explanation, worked examples and collaborative practice enabled students to learn the procedure, while the game scenario supplied a concrete reason for using it. The purpose of the progression was to connect the mathematical mechanisms to the communication constraints they address, rather than to treat them as unrelated calculations. The final mission functioned as an integrative competitive application of the mechanisms introduced during the preceding learning phases. Competing teams had to guide their fleets along assigned multi-leg routes while communicating through the Game Master-controlled observable channel. Mission conditions determined which previously learned procedure had to be applied to each command. Successful movement therefore depended on representing commands efficiently where message length was constrained, recovering them when the channel was disturbed and applying encryption when confidentiality was required.

2.3. *Collaborative activity and individual assessment*

Collaboration allows students to negotiate representations, check calculations and coordinate decisions, but successful team performance is not evidence that every member has mastered each procedure. The module therefore concluded with an individual 100-point examination.

Conceptual domain	**Operational role in the game**	**Individual examination task(s)**
Entropy and source coding	Command distributions and message-length constraints motivate efficient representation through entropy, Huffman coding and arithmetic coding.	Tasks 1–3: entropy calculation and interpretation; Huffman coding and average code length; arithmetic encoding and decoding.
Binary command encoding and Hamming protection	Direction and distance are converted into a binary command representation. A controlled single-bit disturbance requires error detection and correction before the fleet can execute the command.	Task 4: binary encoding of a command, Hamming (11,7) protection, error detection/correction, and recovery of the decoded command.
Reed–Solomon encoding and decoding	A command is represented by finite-field symbols and supplemented with redundant symbols. Controlled symbol errors require reconstruction of the original message before movement can occur.	Tasks 5–6: construction of the message polynomial and transmission symbols; Reed–Solomon decoding, error identification and message recovery.
Key exchange and confidentiality	Because the channel is observable to the opposing team, headquarters and fleet establish a shared value and use it to encrypt a command before transmission.	Task 7: Diffie–Hellman shared-key calculation, XOR encryption process, and encrypted message.

Table 1. Alignment of information-theory concepts, game mechanics, and individual examination tasks

Note: This table documents the intended alignment between game activities and examination domains. It does not demonstrate that participation in a mission caused individual learning. The final examination provides evidence of individual post-module performance, but not of learning gain or the causal effect of the game.

Working Paper of 37th DAAAM Symposium

It required each student to calculate, apply and explain entropy, Huffman and arithmetic coding, Hamming protection, simplified Reed-Solomon coding, Diffie-Hellman key exchange and XOR encryption without team support. To reduce direct answer copying among students seated in small groups, five examination variants were used. Each variant contained the same task structure, conceptual domains and point allocation, but used different numerical parameters, messages and code instances.

3. Pilot implementation and method

The game was implemented during a five-day Erasmus+ international module on information theory and secure communication. The cohort included students from higher-education institutions in Croatia, Germany, Georgia, Lithuania and Spain, with heterogeneous study programmes, semesters of study and previous exposure to relevant mathematical and technical concepts.

Nineteen students completed the individual final examination. Eighteen had also completed the entry-profile questionnaire and were included in descriptive comparisons between domain-specific self-reported familiarity and examination performance. The study was a design-and-pilot implementation study conducted in an authentic intensive-module setting, not a controlled intervention study. During gameplay, students worked in competing teams with physically separated headquarters and fleet roles. The implementation used five boards: two headquarters boards, two fleet boards and a reference board controlled by the Game Master. This arrangement prevented direct visual access to other roles' operational information and made mediated communication necessary for action. All messages, however, remained observable on the shared communication channel. The final examination was completed individually.

Two data sources were used: an entry-profile questionnaire and an individual final examination. The questionnaire was administered before the module and used 1–9 domain-specific self-reported familiarity ratings for concepts including entropy, Huffman and arithmetic coding, Hamming codes, XOR operations, modular arithmetic, Diffie-Hellman key exchange, Galois fields and Reed-Solomon coding. Because it relied on self-report and did not require students to solve problems equivalent to those in the examination, it was not treated as a pre-test from which learning gain could be estimated.

The final examination comprised seven tasks worth 100 points. It assessed entropy; Huffman coding and average code length; arithmetic coding and decoding; binary command encoding and Hamming protection; Reed-Solomon encoding and decoding; and Diffie-Hellman key exchange with XOR encryption. Five parameterised variants assessed the same conceptual domains with different numerical values and message instances. They were used to reduce direct copying among students seated in small groups, not as psychometrically equivalent forms for statistical comparison. For item-level analysis, scores were aggregated into four domains: compression performance (entropy, Huffman coding and arithmetic coding; 45 points); binary encoding and Hamming protection (15 points); Reed-Solomon performance (25 points); and key-exchange performance (15 points).

The analysis is exploratory. The small sample, subjective entry measure, absence of an objective parallel pre-test and absence of a comparison condition prevent estimation of learning gain or the causal effect of the game. Examination performance may reflect the combined contribution of prior knowledge, instruction, guided work, peer interaction, learning materials and the game design. Moreover, although examination variants reduced direct copying, students completed them in a co-located setting; the results should therefore be interpreted as individually recorded performances rather than fully independent observations.

4. Results

Nineteen students completed the individual final examination. Scores ranged from 0 to 100 points (M = 73.3, SD = 30.7, Md = 88); twelve students (63.2%) achieved at least 80 points. The difference between the mean and median reflects a small number of very low scores. Table 2 shows performance by examination domain. Compression and key-exchange tasks had the highest proportional mean scores (77.1% and 78.9%, respectively). Reed-Solomon tasks had the lowest proportional mean score (61.7%), while Hamming/binary and Reed-Solomon results showed substantial variation across students. The Hamming/binary domain had a median of 15 points but six zero scores, indicating heterogeneous rather than uniformly moderate performance. Reed-Solomon tasks also showed substantial variation, particularly in procedures involving polynomial construction and reconstruction. The polarised Hamming results should not be interpreted as evidence that Hamming coding was uniformly difficult. They may reflect heterogeneous prior preparation, engagement, attendance, practice time, or assessment behaviour in the intensive-module setting. These factors were not measured in the present pilot.

Working Paper of 37th DAAAM Symposium

Examination domain	Maximum	Mean (SD)	Median	Mean (%)	Full score	Zero score
Compression: entropy, Huffman and arithmetic coding	45	34.7 (14.6)	40	77.1	8	1
Binary encoding and Hamming protection	15	10.0 (7.1)	15	66.7	12	6
Reed-Solomon encoding and decoding	25	15.4 (9.7)	15	61.7	7	4
Diffie-Hellman key exchange and XOR encryption	15	11.8 (5.6)	15	78.9	13	3

Table 2. Performance by examination domain (N = 19)

Note: Scores are based on the individual final examination (N = 19). Full and zero scores indicate the number of students who achieved the maximum or no points within the respective examination domain.

The entry-profile responses also show a marked discrepancy between perceived prior familiarity and subsequent examination performance. Thirteen of the eighteen respondents rated their familiarity with Reed–Solomon coding between 1 and 3 on the 1–9 scale. Of these students, five achieved at least 20 of 25 points in the Reed–Solomon examination tasks, including three maximum scores. Similarly, twelve respondents rated their familiarity with Diffie–Hellman key exchange between 1 and 3; six of them achieved the maximum score in the Diffie–Hellman/XOR domain. This pattern is compatible with learning during the module and is particularly relevant because the examination required individual execution of procedures practiced in the game. It does not, however, quantify learning gain or isolate the contribution of the game from instruction, materials and peer collaboration. Table 3 indicates that advanced mathematical and cryptographic prerequisites were perceived as weak before the module. Between 66.7% and 83.3% of respondents rated their familiarity with modular arithmetic, Galois fields, Reed–Solomon coding and Diffie–Hellman exchange between 1 and 3. These ratings describe self-reported familiarity before the module rather than objectively measured prior competence.

Concept	What the entry rating assessed	Mean entry rating (1–9)	Median entry rating (1–9)	Students rating 1–3, n (%)
Modular arithmetic	Ability to apply modular arithmetic	2.72	2.0	13 (72.2%)
Galois fields	Understanding of Galois fields	2.17	2.0	15 (83.3%)
Reed–Solomon coding	Understanding of Reed–Solomon coding	2.94	3.0	13 (72.2%)
Diffie–Hellman key exchange	Understanding of the Diffie–Hellman algorithm	3.06	2.5	12 (66.7%)

Table 3. Domain-specific self-reported familiarity with advanced concepts assessed in the final examination (N = 18)

Note: Ratings used a 1–9 self-report scale; 1–3 indicate no understanding or recognition without the ability to explain the concept, whereas 7–9 indicate the ability to explain and apply it.

5. Discussion

The contribution of the physical mission-based collaborative learning game does not lie in adding competition or rewards to conventional exercises. It lies in the design of a distributed operational situation in which headquarters and fleet roles are physically separated, communication is necessary for action, and the transmission channel is observable to the opposing team. A team must formulate a command, represent it, apply the procedure specified by the mission, transmit it and recover its operational meaning before it can act. Source-coding procedures address efficient representation of commands; Hamming and Reed-Solomon coding address recovery from introduced transmission errors; and Diffie-Hellman exchange with XOR encryption addresses confidentiality on an observable channel. The game is therefore not merely gamification in the sense of adding competition or rewards to unchanged exercises [7]. Its mechanics create a reason to use each procedure, while formal instruction and guided practice remain necessary for learning the procedures themselves. The individual examination shows that many students could complete integrated tasks in compression and key exchange after the module, but performance was heterogeneous. The lower and more variable results in Hamming/binary and Reed-Solomon tasks identify these domains as priorities for more explicit scaffolding and diagnostic practice in a subsequent version of the module. These patterns do not identify their own cause: performance may reflect prior mathematical preparation, the amount and quality of practice, task demands, instruction, peer interaction or the game design. The discrepancy between low self-reported familiarity and high subsequent individual scores is compatible with

Working Paper of 37th DAAAM Symposium

learning during the module, but it does not quantify learning gain or show that the game was more effective for particular students. The pilot demonstrates that the game can be implemented in an intensive international module and paired with an individual integrated examination. It does not estimate learning gain or the causal effectiveness of the game. The entry measure was self-reported and not equivalent to the examination; no active comparison condition was used; the cohort was small and heterogeneous; and the parameterised examination variants were not psychometrically equated. The study should therefore be read as a documented design-and-pilot assessment whose value lies in specifying a learning-game architecture and identifying the design of a stronger subsequent evaluation.

6. Conclusion and Future Research

This paper presented a physical mission-based collaborative learning game for information theory and secure communication. Its design links source coding, error-control coding and cryptographic procedures to a common operational problem: teams must exchange commands accurately across physically separated headquarters and fleet boards while communicating over an observable channel. The pilot showed that this design can be implemented in an intensive international module and paired with an individual examination of the relevant procedures. Performance patterns identified lower and more variable outcomes in Hamming/binary and Reed-Solomon tasks, providing a basis for refining scaffolding and practice materials. The pilot does not, however, establish learning gain or the causal effectiveness of the game. A subsequent study should evaluate the complete learning design with a larger multi-cohort sample, objective parallel pre- and post-tests, and an active comparison condition receiving the same content and instructional time through guided problem solving without the mission-based game. Assessment should also include transfer tasks that require students to select and justify an appropriate communication mechanism in a new scenario, as well as a delayed post-test of retention. Such a design could test whether organising compression, error control and confidentiality as interdependent responses to communication constraints improves students' understanding of when and why these mechanisms are needed.

Acknowledgments

The authors gratefully acknowledge Algebra Bernays University, and particularly its International Cooperation Office, for the opportunity to develop and pilot this mission-based collaborative learning game within the Erasmus+ KA131 Blended Intensive Programme.

References

[1] Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, Vol. 27, No. 3, pp. 379-423, ISSN 0005-8580, DOI 10.1002/j.1538-7305.1948.tb01338.x

[2] Huffman, D. A. (1952). A method for the construction of minimum-redundancy codes. Proceedings of the IRE, Vol. 40, No. 9, pp. 1098-1101, ISSN 0096-8390, DOI 10.1109/JRPROC.1952.273898

[3] Rissanen, J. & Langdon, G. G., Jr. (1979). Arithmetic coding. IBM Journal of Research and Development, Vol. 23, No. 2, pp. 149-162, ISSN 0018-8646, DOI 10.1147/rd.232.0149

[4] Hamming, R. W. (1950). Error detecting and error correcting codes. Bell System Technical Journal, Vol. 29, No. 2, pp. 147-160, ISSN 0005-8580, DOI 10.1002/j.1538-7305.1950.tb00463.x

[5] Reed, I. S. & Solomon, G. (1960). Polynomial codes over certain finite fields. Journal of the Society for Industrial and Applied Mathematics, Vol. 8, No. 2, pp. 300-304, ISSN 0368-4245, DOI 10.1137/0108018

[6] Diffie, W. & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, ISSN 0018-9448, DOI 10.1109/TIT.1976.1055638

[7] Deterding, S.; Dixon, D.; Khaled, R. & Nacke, L. E. (2011). From game design elements to gamefulness: defining gamification, Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, 28-30 September 2011, Tampere, Finland, pp. 9-15, ACM, New York, ISBN 978-1-4503-0816-8, DOI 10.1145/2181037.2181040

[8] Perutka, K. & Vymazal, M. (2021). Application of game-based learning in MATLAB using object-oriented programming, Proceedings of the 32nd DAAAM International Symposium, 28-29 October 2021, hosted from Vienna University of Technology, Vienna, Austria, EU, Vol. 32, No. 1, ISBN 978-3-902734-33-4, ISSN 1726-9679, Katalinic, B. (Ed.), pp. 22-32, DAAAM International Vienna, Austria, DOI 10.2507/32nd.daaam.proceedings.004

[9] Plass, J. L.; Homer, B. D. & Kinzer, C. K. (2015). Foundations of game-based learning. Educational Psychologist, Vol. 50, No. 4, pp. 258-283, ISSN 0046-1520, DOI 10.1080/00461520.2015.1122533

[10] Biggs, J. (1996). Enhancing teaching through constructive alignment. Higher Education, Vol. 32, pp. 347-364, ISSN 0018-1560, DOI 10.1007/BF00138871

[11] Wouters, P.; van Nimwegen, C.; van Oostendorp, H. & van der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. Journal of Educational Psychology, Vol. 105, No. 2, pp. 249-265, ISSN 0022-0663, DOI 10.1037/a0031311

Working Paper of 37th DAAAM Symposium