Toward new combinatorial structures using a roundabout model with security related applications

L. N. KISS [(*)]

[(*)]*Faculty of Business Administration, Operations and Decision Systems Department at Université Laval*
2325, rue de la Terrasse, Quebec (Qc) G1V 0A6 Canada
Email: laszlo.kiss@fsa.ulaval.ca

"When the fact encountered does not concur with an accepted theory, one must accept the fact and abandon the theory" (translation). **Claude Bernard.** (1813-1878)

Abstract

This modeling-oriented research focuses on the "physical look" of combinatorics output. It is a well known, simple triviality that for combinations without repetitions of n elements taken k = 2 elements at a time, the output contains only items where the exhaustive meetings property prevails. The questions automatically arises as to how to exploit this promising property in the technological field of operations research, and how to modelize and generalize items to algorithmically obtain outputs with the exhaustive meetings property. We believe that our work will find answers to these conceptual questions.

Let k be any positive integer representing the k rows of a matrix having n columns chosen as a function of k such that n = k (k-1)+ 1. It is possible to rotate each row of the matrix to satisfy the following strong constraint: in the distribution of k-tuple column-vectors obtained by rotations, elements of the matrix meet others once and only once in each column, taking into account the simultaneous presence of k to k elements in the columns. While it is true that the above constraint is concordant with the Golomb Ruler referring to a set of non-negative integers such that no two pairs of distinct numbers from the set have the same difference, this same strong constraint does not limit us solely to finding a shorter Golomb Ruler in order to be able to open the horizon towards new and broader fields of application such as the manufacturing of high security spherical locks and promising encryption-decryption processes, for example. In addition to these potential applications, I will also present my pseudo-genetic roundabout algorithm, and a more in-depth theoretical overview.

Keywords*: pseudo-genetic algorithm, exhaustive meetings property, k amplitude Hamiltonian matrix, contraction, dilatation*

1. INTRODUCTION

This research explores a latent property of combinations without repetition, namely the possibility of shelling k-tuples that satisfy the exhaustive meetings (EM) criterion. The origin of my research goes back to 1994 when I was facing a decision science-related problem in the field of operations research (to establish a mutually acceptable consensus among a group of decision makers) [7]. To date, EM properties have not been explicitly discussed in the literature. Nowhere is there to be found a description of the related algorithmic designs where one might obtain the k-tuples satisfying the EM criterion. Combinations have a long and colourful history and there is a wealth of literature that branches out into many exploratory directions. The corresponding theorems are well known, which is why I do not have to present an elegant overview of the state of the art. Yet I must respectfully pay tribute to the Genius of the number theory (P. Erdos[1], P.Turan, S. Sidon) (dare I say their names), as well as to the fundamental contributions made in the field of finite geometry (mainly E.Galois and the other as J.W. Hirschfeld [11]., C.W.H. Lam, P. Debrowski) [12].. Now to focus immediately on the description of the essential of my rotation model: considering the technical and technological orientation of my intended application, it is not really appropriate to obtain the perfect or optimal Golomb ruler. Since my roundabout algorithm (written in Intel Visual Fortran 10.0) meets the EM criterion through multiple solutions, each solution ("optimal" or not, "perfect" or not) is useful and applicable technologically.

2. The most important security requirements for any system to protect

Security is the core concern behind any cryptosystem, since hacking or computer intrusion is an ongoing and pervasive problem. The particular application of my roundabout system (RS) intentionally dissimulates the descriptions of all fundamental keystones of security, namely authentication, non-repudiation, integrity, confidentiality and auditability, valued properties considered without exception in the field of computer system security.

2.1 Purpose of this RS

The purpose of the RS is to prevent intentional attacks on the activation systems of military devices by intruder spies and inadvertent activation by unauthorized users, even if said individuals are members of the organization (for example, prevention of a missile firing), and to prevent the reading of confidential messages (military, diplomatic, financial, strategic management etc.) by unreliable people.

2.2 Substance of the RS

Let k be any positive integer representing the k rows of a matrix having n columns chosen as a function of k such that $n = k^2 - k + 1$.

Elements $1, \ldots, k^2 - k + 1 \in \mathbb{N}$ constitute the row vectors $v_{[n]}^{(j)}$, $j = 1, \ldots, k$ of base, (i.e., generator) set $\mathbf{B}_{[k \cdot n]}$, while k represents the cardinality of each $k^2 - k + 1$ sub-set $\beta_{[k]}^{(i)}$; $i = 1, \ldots, n$ specifically (i.e., the columns of generator matrix $\mathbf{B}_{[k \cdot n]}$). Consider the following generator matrix:

$$\mathbf{B}_{[k \cdot n].} \equiv \bigcup_{i=1}^{n} \left(\beta_{[k]}^{(i)} \right) \equiv \bigcup_{j=1}^{k} \left(v_{[n]}^{(j)} \right)$$

Note also that between k and n, the inverse relationship that may be established adjusts itself properly to Hoerl's regression [3], [4] if $n = (k^2 - k + 1)$ as follows:

$$k \cong (1.2058438) \cdot \left(1.000136^{n}\right) \cdot \left(n^{0.4661741}\right) \text{ (Hoerl's regression)}$$

Since this regression rarely provides an integer value for k, it is necessary to perform the following operation to calibrate the integer value for k, namely:

If $k - \lfloor k \rfloor > 0.5$, then $k = \lfloor k \rfloor + 1 \equiv \lceil k \rceil$

(then k is rounded off to the closest greater integer value).

If not $k = \lfloor k \rfloor$.

(then k is rounded off to the closest lower integer value).

Considering these preliminary remarks, one can address the following great and complex combinatorial problem:
Among all k-tuples that may be formed through $\binom{n}{k}$ combinatorial analysis, there exist k times k-tuples n < $\binom{n}{k}$ that stand out by reason of strict compliance with the following strong constraints:

2.3 Premises

— In the distribution of these specific k-tuples, each element of 1 to k^2 - k +1 meets another element once and only once, taking into account the simultaneous presence of k to k elements in vectors $\beta_{[k]}^{(i)}$; i =1,…, n (i.e., the columns of $\mathbf{B}_{[k \cdot n)]}$)
In other words, between any vector

$$Card\left\{ \beta_{[k]}^{(i_1)} \bigcap \beta_{[k]}^{(i_2)} \right\} \leq 1;\ i_1 \neq i_2 \text{ et } i_1, i_2 = 1,...,n; \forall i_1, i_2 \in \mathbf{B}_{[k \cdot\ n]}$$

— The frequency of appearance of $\mathbf{B}_{[k\ n]}$ elements is balanced uniformly and equal to k (i.e., once in each row).
Naturally, these strong constraints also allow the formulation of other interpretations, for example:
— Among $\binom{k}{2}$ couples considered at the level of each $\beta_{[k]}^{(i)}$; i = 1,…, n, there are no couples with the same difference;
— Consequently, none of these couples define the same distance. Without getting into finite geometry, which is not my speciality, one can nonetheless literally add the following elementary and trivial interpretations as follows:
— The k-tuples of columns $\beta_{[k]}^{(i)}$ represent straight lines where each line contains k points;
— The points are present once and only once in each row of $\mathbf{B}_{[k \cdot n]}$.

3. ROUNDABOUT MODEL

Thus, it is possible to effect rotations on each row of matrix $\mathbf{B}_{[k \cdot n]}$ to meet the following strong constraint:

In the distribution of specific k-tuples obtained by rotations, elements of the matrix meet once and only once in each column (in other words, exhaustive encounters constellation), considering the simultaneous k to k presence in the columns. Note that the strong constraints concur partially with the Golomb Ruler [2], [8] concerning a set of non-negative integers such that no two distinct pairs of numbers from the set have the same difference. However, the premises (strong constraints) do not limit one solely to finding a shorter Golomb Ruler in order to open the horizon towards new and broader fields of application such as organizing the execution of experimental design, manufacturing high security locks or the equitable distribution of humanitarian aid and protect confidential messages (military, diplomatic, financial etc.) for example.

Therefore, the model involves differences in Φ_i spaces in front or differences in n -Φ_i spaces in back that may be expressed by the equation

$$x_i \big| \rightarrow x_i + \Phi_i \text{, or by}$$

$$x_i \big| \rightarrow x_i - n - \Phi_i .$$

Columns

Rows

rotations	colonnes →	$\beta_{[k]}^{(1)}$	$\beta_{[k]}^{(2)}$		$\beta_{[k]}^{(i)}$	$\beta_{[k]}^{(i+1)}$		$\beta_{[k]}^{(k^2-k+1)}$	lignes ↓
Φ_1	↻	1	2	- - -	i	i+1	- - -	k^2-k+1	$\mu_{[k^2-k+1]}^{(1)}$
⋮	⋮			- - -			- - -		⋮
Φ_j	↻	Φ_j+1	Φ_j+2	- - -	k^2-k+1	1	- - -	Φ_j	$\mu_{[k^2-k+1]}^{(j)}$
⋮	⋮	⋮	⋮		⋮	⋮		⋮	⋮
Φ_k	↻	Φ_k+1	Φ_k+2	- - -	k^2-k+1	1	- - -	Φ_k	$\mu_{[k^2-k+1]}^{(k)}$

Figure 1: Synopsis of the matrix $B_{[k \cdot n]}$

Rows $\mu_{[n]}^{(j)}$; j =1,…,k of $\mathbf{B}_{[k\cdot n]}$ are rotated successively, but to make the algorithm more efficient and as rapid as possible, the following initializations are applied to the Φ_j counters of row rotations:
$\Phi_1 = 0$, namely, the first row does not rotate;

$\Phi_2 \geq \Phi_1+1;$
$\vdots$
$\Phi_j \geq \Phi_{j-1}+1;$

$\vdots$
$\Phi_k \geq \Phi_{k-1}+1;$

As well as $0 < \Phi_j \leq n-1;\ \forall j,\ j = 2,\cdots,k$.
These tactics serve to reduce useless controls to the minimum during propagation of the algorithm.

3.1 Algorithm description (pseudo-genetic algorithm)

First of all, I want to clarify, that my applied algorithm is a computationally intensive pseudo-genetic algorithm. I wrote the codes in Intel Visual Fortran 10.0 **.** This language perfectly satisfies necessary computations rapidity.
∗It is computationally intensive, because the input data quantity is minimal, (which is only two integers k and n), compared to the many numbers of cycles and the checks performed during the algorithm's execution.
∗It is pseudo-genetic, because the problem under discussion:
- Is not a simulation problem;
- Does not fall within "typical" problems generally handled by genetic algorithms (for example, moving a robot, social behaviour, etc.);
- The elitist principle is not applied to selections, since all rotations satisfying the EM criterion are transferred automatically to the next population (i.e., to the next row of the matrix $\mathbf{B}_{[k\cdot n]}$.to process).
- The concept of probability is in no way considered.

First, I seek and preserve values of Φ_2 where the strong constraints between the first and second rows are not violated. Note that at the very onset of the analysis, each of the rotation positions of the second row meets the conditions imposed on exhaustive encounters, because the first row does not rotate. Possible values of Φ_2 represent efficient genes offered as a "heritage" to find appropriate rotations for the third row. Therefore, I save the values of Φ_3 wherein desirable exhaustive encounters between the first, second and third row are not violated. Possible values of Φ_3 once again represent efficient genes offered as a "heritage" to find appropriate rotations for the fourth row, and so on until the analysis of the k –nth row (last row). My algorithm scans columns produced during each rotation attempt and constantly verifies and records the number of each 2 on 2 encounter.
This algorithmic mechanism requires a quadratic working matrix $\mathbf{F}_{[n\cdot n]}$ to record and verify encounter frequencies. However, this quadratic matrix can easily cause the saturation of computer memory in the event of k > 14 values (personal experience on my own computer). To avoid this major technical problem, I used a character string image instead of $\mathbf{F}_{[n\cdot n]}$ quadratic matrix. This change did not hinder the processing of large-scale problems at all, although the conversion into character strings did slow down the processing speed somewhat.
A rotation in the anti-trigonometric direction $\Phi_j \neq 0$ (i.e. clockwise) on a given row $\mu_{[n]}^{(j)}$ of $\mathbf{B}_{[k\cdot n]}$, may be presented schematically as follows:

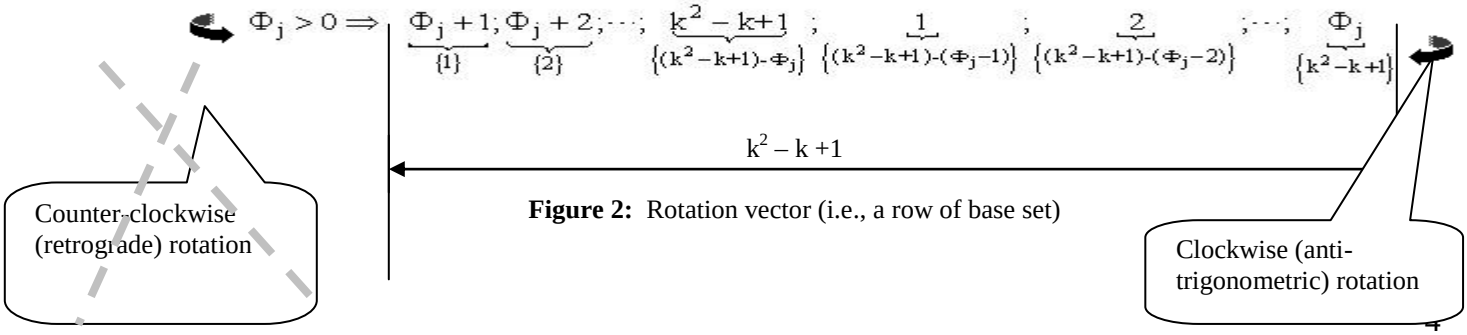

Figure 2: Rotation vector (i.e., a row of base set)

One can easily see that by producing a rotation (clockwise) $\Phi_j \neq 0$ on the j – nth row, the first Φ_j elements at the tail of the row constitute elements 1,2,…, Φ_j, while the head of the row will change to Φ_j+1, Φ_j+2,…, $k^2 - k + 1$ over a length of $(k^2 - k + 1) - \Phi_j$.

The algorithm seeks adequate rotations for each k row positioned above another in order to meet the strong constraints imposed.

Figure 3 summarizes some of the results obtained using my algorithm. Given the multiple solutions obtained, for given k and n, this algorithm might be applied not only for the dissimulation of confidential messages, but also to a range of applications in the field of technology and to problems related to operations research and management.

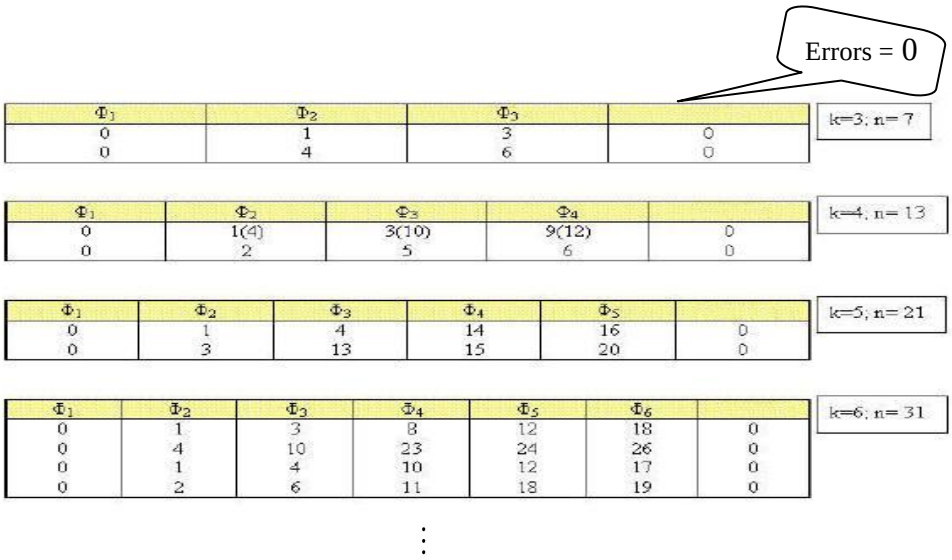

Figure 3: Rotations resulting exhaustive meetings of $B_{[k \cdot n]}$'s elements

4. SOME THEORETICAL CONSIDERATIONS (under the perpetuity of the relative positions principle)

Based on the algorithmic explorations, one can now formulate the following, formally unproven proposals (under the principle of the perpetuity of relative positions). However, the exactitude of these proposals may be verified appropriately by immediate discernment. However, it is not impossible that more formal and most elegant mathematical proofs might be prepared by someone in the future.

Proper rotation of rows of matrix $B_{[k \cdot n]}$ results in a k amplitude Hamiltonian(*) matrix, illustrated in Figure 4.

The particularity of this Hamiltonian matrix $H^{(k)}_{[k \cdot n]}$ allows us to establish various encryption and decryption rules [10] to protect secret messages.

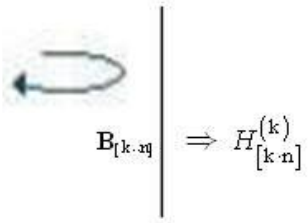

Figure 4: "Metamorphosis" by rotation of the matrix $B_{[k \cdot n]}$ to k amplitude Hamiltonian matrix(*)

Note(*): A k amplitude Hamiltonian matrix exists if the control signal can move through nodes exhaustively while simultaneously and necessarily controlling k nodes at the same time.

Conjecture 1

Since the optimal rotations vector $\Phi^{*}_{[k]}$ satisfies the strong EM constraints imposed, then the complementary rotations vector on $k^2 - k + 1$, i.e. $\Phi^{c*}_{[k]} = n - \Phi^{*}_{[k]}$ also meets the strong EM constraints imposed.

Proof
Through immediate discernment, since both the clockwise and complementary counter-clockwise rotations maintain the structure obtained in $\mathbf{B}_{[k \cdot n]}$ and can only result in the same joint constellations for columns $\beta^{(i)}_{[k]}$
Q.e.d.

Conjecture 2

Once the rotation has transformed the generator matrix $\mathbf{B}_{[k \cdot n]}$ into an k- amplitude Hamiltonian matrix , $H^{(k)}_{[k \cdot n]}$ the number of columns of the latter may extend to infinity, while the EM structure property remains maintained.
The perpetuity of the relative positions principle invites us to add even more depth to the following explanations:

The length $\lambda \equiv n$ of each row $\mu^{(j)}_{[n]}$; j = 1,…k of $\mathbf{B}_{[k \cdot n]}$ can vary between the lower bound and the possible upper bound of the base set, therefore $n_{low..} \leq \lambda \leq n_{upp.}$ or, more explicitly,

- Contraction

$$n_{low.} = \begin{cases} Max\ \Phi_j + 1 \in \Phi^{*}_{[k]};\ j = 1,...,k \\ \text{or alternatively on the complementary vector} \\ Max\ \Phi^{c}_j + 1 \in \Phi^{c*}_{[k]};\ j = 1,...,k \end{cases}$$

- Dilatation

$$n_{upp} \geq \binom{n}{k} \rightarrow \text{but it may tend to } \infty$$

Proof
Through immediate discernment, since we know the principle of the perpetuity of the relative positions (elementary obviousness), consequently the number of columns of the matrix $H^{(k)}_{[k \cdot n]}$ may tighten up to $Max\ \Phi_j + 1$, or $Max \Phi^{c}_j + 1$ or may expand to infinity, without causing the collapse of the established structure and without violating the EM property.
Q.e.d

This wealth of parameters may be illustrated as concentric orbits wherein the black coloured perimeter in bold print represents the generating orbit of length $\lambda = n$, which serves solely to define the vector of optimal rotations $\mathbf{\Phi}^{*}_{[k]}$. Once $\mathbf{\Phi}^{*}_{[k]}$ is defined, the strong constraints are always met if one applies the same $\mathbf{\Phi}^{*}_{[k]}$ to all varied, i.e., contracted, dilated perimeter orbits λ (see Figure 5).

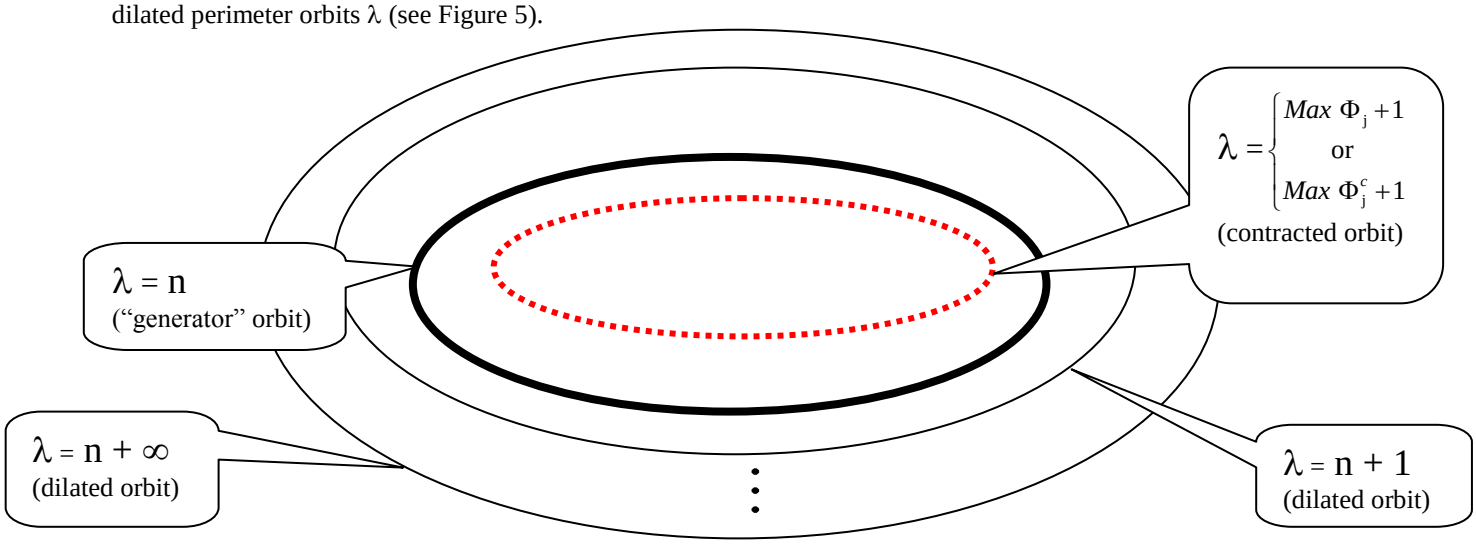

Figure 5: Contraction and Dilatation of Rotation Perimeters

5. DIDACTIC ILLUSTRATION

Consider the structure $\mathbf{B}_{[3x7]:}$ i.e., let n = 7 and k = 3, it is well known that $\binom{n}{k}=\binom{7}{3}=35$; among these 35 triplets can be found 7 times triplets without repetition from 7 elements satisfying the EM criterion (see the triplets on which the red arrows point in Figure 6) . There are always 7 triplets resulting from rotations where the frequency of mutual encounters of elements is strictly equal to one.

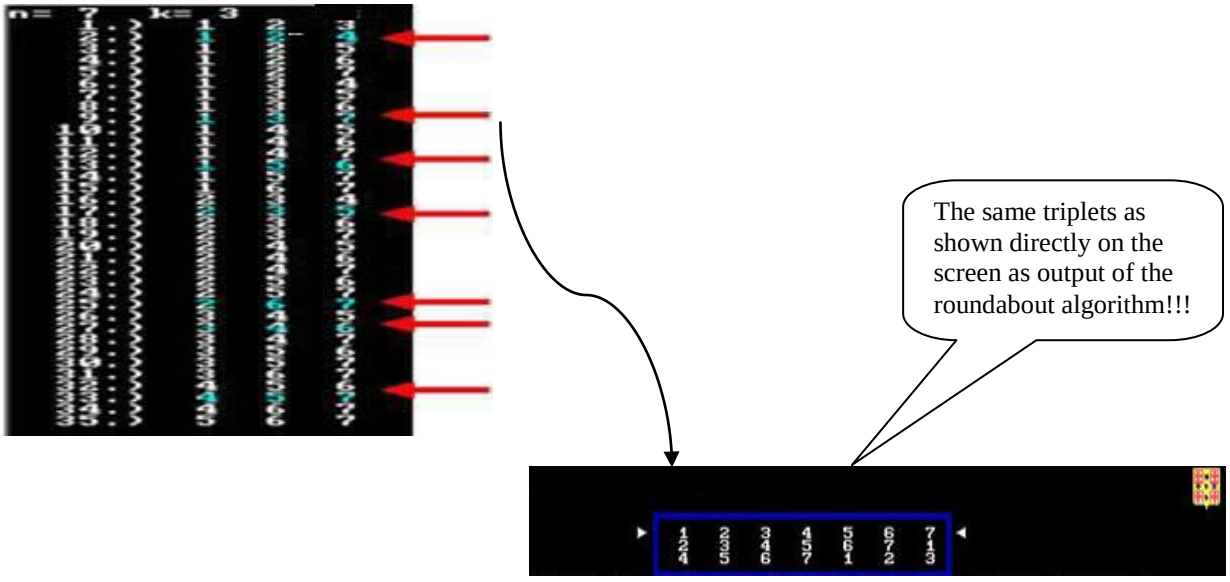

Figure 6: Simultaneous presence among the specific triples of combinations without repetitions that have the exhaustive meetings property.

$\Phi_1^*\left(\mu_{[7]}^{(1)}\right)=0\rightarrow\ 1\ 2\ 3\ 4\ 5\ 6\ 7$, i.e., the first row does not rotate;

$\Phi_2^*\left(\mu_{[7]}^{(2)}\right)=1\rightarrow\ 2\ 3\ 4\ 5\ 6\ 7\ 1$, i.e., the second row must clockwise rotate one step;

$\Phi_3^*\left(\mu_{[7]}^{(3)}\right)=3\rightarrow\ 4\ 5\ 6\ 7\ 1\ 2\ 3$, i.e., the third row must clockwise rotate three steps.

Note that the solution presented about the structure $\mathbf{B}_{[3\cdot7]:}$ is not unique, since complementary rotations also meet the strong constraints of exhaustive encounters. Therefore, complementary rotations represented below also represent a solution (refer to *Conjecture 1*, presented earlier):

$\Phi_1^{c*}\left(\mu_{[7]}^{(1)}\right)=0\ \rightarrow\ \ \ 1\ 2\ 3\ 4\ 5\ 6\ 7$

$\Phi_2^{c*}\left(\mu_{[7]}^{(2)}\right)=7-1=6\rightarrow\ 7\ 1\ 2\ 3\ 4\ 5\ 6$ (complementary rotations)

$\Phi_3^{c*}\left(\mu_{[7]}^{(3)}\right)=\ 7-3=4\rightarrow\ 5\ 6\ 7\ 1\ 2\ 3\ 4$

Then it can be applied to the contraction as well as the dilatation of n, maintaining the same rotations; in other words, n can be contracted to 3 +1 = 4, since $\Phi_{\max}=\Phi_3^*\left(\mu_{[7]}^{(3)}\right)=\ 3$ or n can be dilated for example to 9, or even up to ∞ depending on the user's wishes (refer to *Conjecture 2*,presented earlier).

1234
2341 (contraction) or 123456789
234567891 $\cdots$ (dilatation)
4123
456789123

For a better understanding, I know more complex examples will be required and well as in-depth written explanations.

6. TWO CONCRETE TECHNOLOGICAL APPLICATIONS (already exceeding the cogitation stage!!!)

6.1 High security spherical-form lock (only brief concept description)

The roundabout model concept allows us to organize k rows $\mu_{[n]}^{(j)}$; j = 1,.., k of matrix $\mathbf{B}_{[k \cdot n]}$ around an axial guide-tube forming the rotating "layers" of the lock. The axial guide-tube might be equipped with two contact shoes for necessary circuitry and concealed communication between poles, and positioned axially and concentrically with the rotating "layers."

The mathematical relationships between the number k of "layers" and the number of possible rotational positions of the "layers" allows the establishment of a particular and simultaneous constellation of layers such that for the total layers, $k^2 - k + 1$ numbers constituting these rotating "layers" are each found in a Hamiltonian position (meaning that if one considers the $k^2 - k+1$ numbers on the layers as nodes, the Hamiltonian position is achieved if it is possible to move through the network of nodes by passing once and only once through each node).

The uniqueness of my lock resides in the additional constraint of the control signal having to move through the network of nodes passing mandatorily through the steps of k nodes at a time, column by column, while meeting the EM criterion. Only in this case will the lock unlock. This cycle is based on the theoretical principle developed by the author of this paper whereby if one considers all non-repetitive combinations of $k^2 - k+1$ elements taken k elements at a time, then among all the k-tuples of $\binom{k^2-k+1}{k}$ that may be formed by $k^2 - k+1$ elements, there exist k-tuples in numbers $k^2 - k+1 < \binom{k^2-k+1}{k}$ that stand apart for their strict compliance with the strong constraints regarding exhaustive encounters of $k^2 - k+1$ numbers (nodes) of each stratum of the lock.

Applications for such a high security lock are simply inestimable. Potential users might be holders of secrets in the Armed Forces, security authorities or any other organization where access to confidential installations is closely monitored.

Likewise, there is also the possibility of an analogical option in the form of a microprocessor (in other words, the EPROM image of the algorithm) for my "strati-form" lock. In this case, the **lock becomes open-ended:** should a non-authorized intruder accidentally discover the proper alignment of one the "layers," the virtual circumference of the other layers will dilate automatically by a random φ factor (invisible, undetectable by the intruder) and the intruder will then face $\varphi \cdot (k^2\text{-}k+1)$ rotation positions for the remaining "layers" (Figure 4 and Conjecture 2 presented earlier prove the **non-violability of the RS** proposed, irrespective of crafty manoeuvres attempted by the intruder spy).

To ensure one and only one encounter at the level of each of n nodes, the magnetism of ferrite (core) rings might be used where 0 and 1 might easily be lodged as two distinct states. Wires to these cores might serve to change the states as well as read current states in order to memorize the states of nodes in the RS.

The RS unlocks only if the system has memorized 1 bit in numbers of

$$\binom{n}{2}.$$

If not, the lock remains locked!

Encryption is obtained automatically by the innate concept of RS, while decryption requires the holder of the secret to carry out "layer" rotations as partially summarized in Figure 3.

To illustrate the inviolability of the proposed lock in terms of time, let us assume that an RS with ten "layers" is attacked by a gifted intruder spy capable of executing one trial and error attempt per second, which is clearly not feasible. The total number of rotation positions to verify is equal to $91^{10} = 3,894161181181108 \cdot 10^{19}$. It is totally impossible for an intruder spy to have this many seconds at his disposal because the number in question is equivalent to the one hundredth of the age of the universe! The illegal "keybreaker" is doomed to fail.

6.2 Dissimulation of confidential messages (only brief synoptic overview)

Proper rotation of rows of matrix $\mathbf{B}_{[k \cdot n]}$ results in a k amplitude Hamiltonian matrix illustrated above in Figure 4.
This last constitutes the main mathematical device around which my dissimulation method is articulated.

The particularity of matrix $H^{(k)}_{[k\cdot n]}$ allows one to establish various encryption and decryption rules [8] to protect secret messages. Substantially, it consists of a particular form of alliance between a protective text and a secret message. The secret message can be inserted character by character either by the Euclidean distance or by angle distance in the protective text's mass. Pictures, diagrams and patterns will be inserted pixel by pixel at these distances from the Hamiltonian matrix. However, the secureware nature of these sketched applications invites the author of this paper to provide more information on the dissimulation processes developed only to a restricted audience.

Note that if requested, the author is disposable to collaborate in the definition of software functionalities and the production of prototype and/or educational software!!!

7. CONCLUDING REMARKS AND FURTHER CONSIDERATIONS

In this study, the EM properties of k-tuples were explored using a rotation model and has-beens applied to two security related technological applications, namely the development of the design of a high security lock as well as the design of an encoding - decoding process. With proper rotations I obtained not only satisfaction of the EM criterion, but also the transformation of the generator matrix $\mathbf{B}_{[k\cdot n]}$ into a matrix known as the k amplitude Hamiltonian matrix $H^{(k)}_{[k\cdot n]}$ The mathematical properties of $H^{(k)}_{[k\cdot n]}$ can open entirely new perspectives in applications, such as the birth of **high security evolutionary locks**, or **high security evolutionary encryption codes.** However, at the present time, one can only imagine their silhouettes and not their full boundaries, because the concrete achievements of this new revolutionary application require additional research efforts from the author and research collaborations with embedded software specialists and automation engineers. However, I am well acquainted with the solidly established mathematical foundation that invites me to effectively prepare my ambitious research program, even though I retired in September 2006.

7.1 SYNOPTIC OVERVIEW OF POTENTIALLY POSSIBLE APPLICATIONS (BOTH IMMEDIATELY AND IN THE NEAR FUTURE)

∗Technological applications

- Encryption-decryption processes
- High security evolutionary locks
- Dissimulating confidential messages by high security evolutionary codes
- Balanced dosage of alloy components in the metal industry

∗Non- technological applications

- Experience plans (identification of manufacturing process parameters)
- Equitable distribution of humanitarian aid (ensuring the fast and fair distribution of aid for persons in need in disaster areas, for example Darfur, victims of a tsunami, etc.)
- Determining the best starting point for the traveling salesman, creating a new design of this well know classic problem)
- Finding the best installation point of a warehouse
- Determining the most efficient control cycles (ground or maritime area), etc.

ACKNOWLEDGMENT

I wish to express my gratitude to my university, namely the Research Department at the Faculty of Business Administration at Laval University (Québec, Canada) for granting me a research grant in the spring of 2013. Although I retired in September 2006, the grant has allowed by to prepare this publication.

REFERENCES

[1] **Erdös,** Paul,**Turan**, Pàl, On a Problem of Sidon in Additive Number Theory, and on some Related Problems *J. London Math. Soc.* 1941 s1-16 (4):p. 212-215

[2] **Golomb, S.W**., "Where to Point the Antennas," *Astronautics & Aeronautics Magazine*, July, 1962.

[3]**Hoerl A.E**., Kennard R.W., "Ridge regression: biased estimation for nonorthogonal problems," *Technometrics* 12, 1970(a), p. 55-67.

[4]**Hoerl A.E**., Kennard R.W., "Ridge regression: applications to nonorthogonal problems," *Technometrics* 12, 1970(b), p. 69-82.

[5] **Babcock. W.C**., *Intermodulation interference in radio systems*, Bell Systems Technical Journal (1953), 63-73

[6] **Ruzsa**, I.Z., *Solving a linear equation in a set of integers I*, Acta Arithmetica, 65 (1993), p. 259-282.

[7] **Martel, J.-M.** and **Kiss, L.N**., *"A Support to Consensus Reaching in Group Decision,"* Group Decision and Negotiation Journal, vol.3, , n ^{o} 1, pp.93-119, (1994).

[8] **Dimitromanolakis, A.**, Analysis of the Golomb Ruler and the Sidon Set Problems, and Determination of Large, Near-Optimal Golomb Rulers, Technical University of Crete, Department of Electronics and Computer Engineering, 2002.

[9] **Erdos, P**. and A. Renyi, Additive properties of random sequences of positive integers, Acta Arithmetica 6 (1960), 83-100

[10]**Schneier, B.** ***Applied Cryptography*****,** Second Edition, John Wiley & Sons, 1996 ISBN 0-471-1170

[11] **Hirschfeld, J.W.P.** ***Finite Projective Spaces of Three Dimensions***
Oxford Mathematical Monographs, 370 pp., 1986

[12] **Dembowski, P.** ***Finite Geometries***
Springer Classics in Mathematics, 1997 reprint of the 1968 edition, 375 pp.