Advances in Science and Technology Research Journal

Advances in Science and Technology Research Journal 2022, 16(4), 243–255
https://doi.org/10.12913/22998624/153086
ISSN 2299-8624, License CC-BY 4.0

Received: 2022.07.22
Accepted: 2022.08.23
Published: 2022.09.01

Constructive Consistent Approximations in Pairwise Comparisons

Ryszard Smarzewski[1], Ryszard Kozera[2,3*]

[1] Institute of Mathematics and Cryptology, Cybernetics Faculty, Military University of Technology, S. Kaliskiego 2, 00-908 Warsaw, Poland

[2] Institute of Information Technology, Warsaw University of Life Sciences – SGGW, ul. Nowoursynowska 159, 02-776 Warsaw, Poland

[3] School of Physics, Mathematics and Computing, The University of Western Australia, 35 Stirling Highway, Crawley, W.A. 6009 Perth, Australia

* Corresponding author's e-mail: ryszard kozera@sggw.edu.pl; ryszard.smarzewski@wat.edu.pl

ABSTRACT

In this paper we investigate groups which admit the existence of weighted consistent approximations for pairwise comparisons matrices. These approximations are defined by extending the classical matrix projection for R_+ to abstract weighted projections on the non-linear sets of transitive group-valued matrices. It is of interest that all of them are represented by general explicit formulae dependent on an abstract logarithmic function. This general approach is applied to the groups Z_p and F_{2^m} m which are of fundamental importance in cryptography. Finally, we use our unified mathematical model of pairwise comparisons for continuous one-parameter unitary groups, which play a fundamental role in physics.

Keywords: cryptography, computer science, applied mathematics

INTRODUCTION

The consistent approximation plays fundamental role in the pairwise comparisons theory and its applications, cf. Saaty [1, 2], Laarhoven and Pedrycz [3], Koczkodaj and Orłowski [4], Cavallo and Brunelli [5], Farkas et al. [6], Koczkodaj and Szarek [7], Holsztyński and Koczkodaj [8], Koczkodaj and Szwarc [9], Koczkodaj et al. [10], Smarzewski and Rutka [11] and other references therein. According to [1, 3, 4] a consistent projection is defined, for the multiplicative group of positive real and triangular fuzzy numbers, as a composition of additively and multiplicatively invariant matrix mappings. On the other hand, in view of important applications of the pairwise comparisons not only in biology, cryptography and physics, but also in psychology [2], it would be interesting to characterize groups, which admit consistent projections. We note that such attempt has been recently done by Wajch [13]. However, several attempts to define a useful consistent approximation in an abstract setting have not been satisfactorily accomplished until now. An assessment of the latter is discussed in a recent work [14].

In this paper we present a class of groups that admit the existence of non-trivial consistent projections. In doing so, in the next section we give conditions that such groups should satisfy and discuss their properties. Among them the most restrictive and important postulate refers to the existence of appropriate logarithmic and exponential functions. As shown in two sections (Consistent Matrices in Pairwise Comparisons and Abstract Consistent Projections) it is hard to overestimate the influence of abstract logarithms on the generic properties of consistent approximations not only of multiplicative but also of additive type. In addition, both sections in question shed light why the theory of pairwise comparisons is not applicable to every group [13].

The class of abstract logarithmic functions includes the discrete logarithms defined for every cyclic multiplicative group. Therefore, it is possible to derive in Abstract Consistent Projections section the explicit formulae for the weighted consistent projections of reciprocal matrices with entries in the multiplicative

groups $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ of remainders modulo a prime number p. In the next section to Abstract Consistent Projections section we establish results of this kind for multiplicative groups $\mathbb{F}_{2^m}^* = \mathbb{Z}_2[x]/w_m(x)$ of all non-trivial polynomials over $\mathbb{Z}_2 = \{0, 1\}$ modulo a fixed primitive polynomial $w_m(x)$ of degree m with coefficients in the field $\mathbb{Z}_2$. This suggests that modular consistent projections may become a useful tool to to design new algorithms and protocols not only for the computer supported pairwise comparisons, but also for data origin authentication of messages M in cryptography (see e.g. Durnoga and Pomykała [15]). Finally, we notice that the groups $\mathbb{Z}_p^*$ and $\mathbb{F}_{2^m}^*$ already play the central role in several fields of computer science such as e.g. cryptography, processing information, discrete Fourier analysis, coding theory, data storage, modular operations or programming languages. An interested reader may also find some related work in Durnoga and Źrałek [16].

Finally, the second last section is an application of the previous sections to develop pairwise comparisons for one parameter unitary groups $U : \mathbb{R} \to \mathcal{B}(H)$ in the algebra of all bounded linear operators from a Hilbert space H into itself. The results presented there demonstrate the power of functional calculus in designing our model of pairwise comparisons, which is based on using the abstract logarithms. In this model, we construct first an auxiliary additive consistent projection of an antisymmetric matrix $[\log U(\alpha_{kj})]_{n\times n}$ onto the group $\mathcal{A}_n(\mathbb{L})$ of all additively consistent matrices with entries in $\mathbb{L} = \log U(\mathbb{R})$. In sequel, we use the abstract exponential function to derive a multiplicative consistent projection of a reciprocal matrix $M = [m_{kj}]_{n\times n}$ with entries $m_{kj} = U(\alpha_{kj})$ onto the group $\mathcal{M}_n(\mathbb{K})$ of all multiplicatively consistent matrices $T = [t_{kj}]_{n\times n}$ with entries in $\mathbb{K} = U(\mathbb{R})$.

DEFINITIONS AND PRELIMINARIES

A classical concept of pairwise comparisons can be formulated for an algebra $\mathcal{A}$ with identity such that $\mathcal{A}$ is also an ordered vector space over a field $\mathbb{F}$ of real numbers. It means that an order relation $\leq$ is defined on $\mathcal{A}$, which is reflexive, transitive and invariant with respect to the operations of addition and multiplication by non-negative scalars in $\mathbb{F}$, but not necessarily antisymmetric [17]. In this paper we assume that the order relation is defined on the algebra $\mathcal{A}$ by the formula

$$x \leq y \quad \text{if and only if} \quad y - x \in \mathcal{A}_+,$$

where $\mathcal{A}_+ \supset \{0, 1\}$ is a wedge (a cone) of positive elements in $\mathcal{A}$ with vertex 0 and identity 1. For the simplicity such an algebra $\mathcal{A}$ will be called ordered.

In the theory of pairwise comparisons there are considered two groups $\mathbb{K}$ and $\mathbb{L}$ in $\mathcal{A}$: $\mathbb{K}$ of multiplicative type and $\mathbb{L} \subset \mathcal{A}$ of additive type. It should be noticed that all pairwise comparisons problems are originally stated for the multiplicative group $\mathbb{K}$. Since these problems are extremely hard to solve even by computers [1], [3], [4], [10] and [11], they are approximated by additive projections onto $\mathbb{L}$-valued consistent matrices, which are eventually transformed by using abstract exponential functions.

Definition 1. Two multiplicative and additive groups $\mathbb{K}$ and $\mathbb{L}$ in an ordered algebra $\mathcal{A}$ are said to be *logarithmically homeomorphic*, if there exists a collection:

$$\Phi(\mathbb{K}, \mathbb{L}) = \{\varphi_\beta : \beta \in G(\mathbb{K})\}$$

of homeomorphisms $\varphi_\beta : \mathbb{K} \to \mathbb{L}$, which have the following properties:

$$\varphi_\beta(xy) = \varphi_\beta(x) + \varphi_\beta(y), \tag{1}$$

and

$$\varphi_\beta(\varphi_\alpha^{-1}(x)) = x\varphi_\beta(\alpha), \tag{2}$$

for all $x, y \in \mathbb{K}$ and $\alpha, \beta \in G(\mathbb{K})$. The homeomorphisms φ_β will be called *abstract logarithms.*

Remark 1. If φ is an abstract logarithm in $\Phi(\mathbb{K}, \mathbb{L})$ then it follows from Definition 1 that the inverse mapping φ^{-1} of $\mathbb{L}$ onto $\mathbb{K}$ has the property:

$$\varphi^{-1}(u + v) = \varphi^{-1}(u)\varphi^{-1}(v),$$

for all $u, v \in \mathbb{L}$. Hence the addition in $\mathbb{L}$ satisfies the formula:

$$u + v = \varphi[\varphi^{-1}(u)\varphi^{-1}(v)].$$

Example 1. The concept of classical pairwise comparisons (see [1], [5], [11] and [18]) in $\mathbb{R}$ is characterized by the following pre-assumptions:

$$\mathcal{A} = \mathbb{F} = \mathbb{R},\ \mathcal{A}_+ = [0, +\infty),\ \mathbb{K} = (0, +\infty),\ \mathbb{L} = \mathbb{R},$$
$$G(\mathbb{K}) = \{\beta : \beta > 0, \beta \neq 1\},\ \Phi(\mathbb{K}, \mathbb{L}) = \{\log_\beta(x) : \beta \in G(\mathbb{K})\}.$$

Note that now condition (2) coincides with the well-known formula

$$\log_\beta(\alpha^u) = u \log_\beta \alpha.$$

Example 2. Consider the finite field $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ in which operations of addition and multiplication modulo a prime number $p > 2$ are introduced. It is clear that $\mathbb{Z}_p$ becomes an algebra if we set $\mathbb{F} = \mathbb{Z}_p$. In this case we propose to choose:

$$\mathcal{A} = \mathbb{F} = \mathcal{A}_+ = \mathbb{Z}_p,\ \mathbb{K} = \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\},\ \mathbb{L} = Z_{p-1},$$

$$\Phi(\mathbb{K}, \mathbb{L}) = \{\log_\beta(x) : \beta \in G(\mathbb{Z}_p^*)\},$$

where $\mathbb{Z}_{p-1} = \{0, 1, \ldots, p-2\}$ is the additive group, under the operation of addition $(x + y)(\mathrm{mod}\,(p-1))$, the set

$$G(\mathbb{Z}_p^*) = \{\beta \in \mathbb{Z}_p^* \setminus \{1\} : \beta \equiv \beta^p (\mathrm{mod}\, p)\}$$

consists of all generators of the multiplicative group $\mathbb{Z}_p^*$ of positive remainders modulo p and $\varphi_\beta(x) = \log_\beta x$ denotes the discrete logarithm of $x \in \mathbb{Z}_p^*$ to the base β which is the unique integer y, $0 \leq y \leq p-2$, such that $\beta^y \equiv x \bmod p$ (see [19]). In particular, if we take $\beta = 10$ in the set $G(\mathbb{Z}_{19}^*) = \{2, 3, 10, 13, 14, 15\}$ of all generators of the multiplicative group $\mathbb{Z}_{19}^*$, then the elements of additive group $\mathbb{Z}_{18}$ of discrete logarithms $y = \log_{10} x$ are as listed in the second row of Table 1. A simple inspection shows that the discrete logarithm $y = \log_{10} x$ is an homeomorphism between the multiplicative group $\mathbb{Z}_{19}^*$ of remainders modulo 19 and the additive group $\mathbb{Z}_{18}$ of remainders modulo 18. In particular for $x = 7$ and $y = 16$ we have:

$$\log_{10}(xy) = \log_{10} 112 \equiv \log_{10} 17\ (\mathrm{mod}\, 19) = 8$$

and also

$$\log_{10} x + \log_{10} y = 12 + 14 \equiv 8\ (\mathrm{mod}\, 18).$$

Table 1. Discrete logarithms $y = \log_{10} x$ in the group $\mathbb{Z}_{19}^*$.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
y	0	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

Remark 2. The finite fields $\mathbb{Z}_p$ and multiplicative groups $\mathbb{Z}_p^*$ are fundamental in applied cryptography. Additionally, in modern applied cryptography a vital role is also played by cyclic groups of rational points on elliptic curves, c.f. Menezes et al. [19], Husemöller [20] and Washington [21]. Consequently, it would be interesting to investigate the concept of consistent approximation in cyclic groups. In the preliminary step, we address below the latter for the multiplicative groups $\mathbb{F}_{2^m}^*$.

Remark 3. Note that the condition (2) from Def. 1

$$\log_\beta(a^x) = x \log_\beta \alpha,$$

remains true for discrete logarithms. For example, if $\alpha = 14$, $\beta = 10$ and $x = 8$, then upon resorting to Table 1 a simple verification yields:

$$\log_\beta(\alpha^x) = \log_{10}(14^8) \equiv \log_{10} 4\ (\mathrm{mod}\, 19) = 16$$

and

$$x \log_\beta \alpha = 88 \equiv 16\ (\mathrm{mod}\, 18).$$

CONSISTENT MATRICES IN PAIRWISE COMPARISONS

As in previous section we suppose that $\mathbb{K}$ is a multiplicative and $\mathbb{L}$ is an additive group in an ordered algebra $\mathcal{A}$ over a field $\mathbb{F}$ having identity 1 and wedge $\mathcal{A}_+ = \{x \in \mathcal{A} : x \geq 0\} \supset \{0, 1\}$. In order to formulate the concept of *real consistent approximations* (cf. e.g. [4], [10] and [1]) in an abstract setting, let $\mathbb{K}^{n\times n}$ be the set of all $\mathbb{K}$-valued matrices $M = [m_{ij}]_{i.j=1}^{n}$ with entries in a multiplicative group $\mathbb{K}$. Then $\mathbb{K}^{n\times n}$ is a multiplicative matrix group under the operation of pointwise multiplication of matrices $M = [m_{ij}]$ and $X = [x_{ij}]$:

$$[m_{ij}] \cdot [x_{ij}] = [m_{ij}x_{ij}].$$

The identity in $\mathbb{K}^{n\times n}$ is matrix $E = [e_{ij}]$ with all entries $e_{ij} = 1$. Similarly, we define the additive group $\mathbb{L}^{n\times n}$ of matrices over an additive group $\mathbb{L}$. In this case the matrix operation is defined by the formulae

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}].$$

Moreover, let $\mathfrak{M}_{n\times n} = \mathfrak{M}_{n\times n}(\mathbb{K})$ be the subset of reciprocal $\mathbb{K}$-valued matrices $M = [m_{ij}]$ for which $m_{ii} = 1$ and

$$m_{ij}m_{ji} = 1 \text{ for every } i, j = 1, 2, \ldots, n. \tag{3}$$

These matrices are called abstract PC matrices. If an abstract PC matrix $M = [m_{ij}]$ satisfies in addition the condition of transitivity:

$$m_{ik}m_{kj} = m_{ij}, \quad \text{whenever } 1 \leq i < k < j \leq n, \tag{4}$$

then such M is called as consistent. At this point we note that the concept of multiplicative consistency should not be identified with its dual analogue of the abstract additive consistency. Indeed, the latter is defined for the additive matrix group $\mathfrak{A}_{n\times n} = \mathfrak{A}_{n\times n}(\mathbb{L})$, which consists of all antisymmetric matrices $A = [a_{ij}]$ with entries in the additive group $\mathbb{L}$. More specifically, a matrix $A = [a_{ij}] \in \mathfrak{A}_{n\times n}$ is called additively consistent if it satisfies the following condition:

$$a_{ik} + a_{kj} = a_{ij}, \quad \text{whenever } 1 \leq i < k < j \leq n. \tag{5}$$

From now on we denote the subgroups of $\mathbb{K}^{n\times n}$ containing all multiplicative and additive consistent matrices by the following symbols $\mathcal{M}_n = \mathcal{M}_n(\mathbb{K})$ and $\mathcal{A}_n = \mathcal{A}_n(\mathbb{L})$.

Theorem 1. *If* $\mathbb{K}$ *and* $\mathbb{L}$ *are logarithmically homeomorphic groups, then the groups:*

$$(a) \quad \mathfrak{M}_{n\times n}(\mathbb{K}) \quad \textit{and} \quad \mathfrak{A}_{n\times n}(\mathbb{L}) \quad \textit{of reciprocal matrices}$$

$$(b) \quad \mathcal{M}_n(\mathbb{K}) \quad \textit{and} \quad \mathcal{A}_n(\mathbb{L}) \quad \textit{of consistent matrices}$$

are also logarithmically homeomorphic. Moreover, each matrix logarithm φ *has the form*

$$\varphi(M) = [\varphi(m_{ij}]_{n\times n},$$

where $M = [m_{ij}]_{n\times n}$ *and* $\varphi(m_{ij})$ *is an abstract logarithm of* m_{ij}.

Proof. If matrix $M = [m_{ij}]$ is reciprocal, it follows from Definition 1 that the matrix A with entries $a_{ij} = \varphi(m_{ij})$ satisfies

$$a_{ij} + a_{ji} = \varphi(m_{ij}m_{ji}) = \varphi(1) = 0.$$

Hence it is antisymmetric. If in addition M is consistent, then the condition of transitivity yields

$$a_{ij} = \varphi(m_{ij}) = \varphi(m_{ik}m_{kj}) = \varphi(m_{ik}) + \varphi(m_{kj}) = a_{ik} + a_{kj}.$$

This completes the proof.

Example 3. The inverses of elements in $\mathbb{Z}_p^*$ can be easily computed by the extended Euclidean algorithm [19]. However, if p is small, then it is preferable to use a corollary to Fermat's theorem, which states that the inverse to β^k is equal to β^{p-1-k}, where β is a generator of $\mathbb{Z}_p^*$ and $k = 0, 1, \ldots, p-1$. For the special case of $p = 19$, all inverses are listed in Table 2, which determines the following positive matrix:

$$M = \begin{bmatrix} 1 & 4 & 11 & 12 \\ 5 & 1 & 17 & 9 \\ 7 & 9 & 1 & 7 \\ 8 & 17 & 11 & 1 \end{bmatrix}$$

as reciprocal. However, in view of the identities $m_{12}m_{24} \equiv 4 \pmod{19}$ and $m_{14} = 12$, the matrix M is not consistent. On the other hand, the congruence $4 \cdot 17 \equiv 11 \pmod{19}$ shows that the following sub-matrix:

$$M_1 = \begin{bmatrix} 1 & 4 & 11 \\ 5 & 1 & 17 \\ 7 & 9 & 1 \end{bmatrix}$$

is multiplicatively consistent.

Table 2. Inverses in the multiplicative group $\mathbb{Z}_{19}^*$.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x^{-1}	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18

ABSTRACT CONSISTENT PROJECTIONS

According to [1, 4, 10, 12] the classical pairwise comparisons theory is based on the approximation of inconsistent matrices by consistent projections. This approach can be extended to groups $\mathcal{M}_n = \mathcal{M}_n(\mathbb{K})$ and $\mathcal{A}_n = \mathcal{A}_n(\mathbb{L})$ of consistent matrices as specified below. For this purpose we note that their elements have the following canonical representations (with products $xy^{-1} \in \mathbb{K}$ written as ratios x/y)

Lemma 1. *If $M = [m_{ij}] \in \mathcal{M}_n$ and $A = [a_{ij}] \in \mathcal{A}_n$ then:*

(a) $m_{ij} = t_i/t_j$, where $t_1 \in \mathbb{K}$ is arbitrary and $t_j = t_1/m_{1j} \in \mathbb{K}$, for every $j = 2, 3, \ldots, n$;

(b) $a_{ij} = s_i - s_j$, where $s_1 \in \varphi(\mathbb{K})$ is arbitrary and $s_j = s_1 - a_{1j} \in \varphi(\mathbb{K})$, for every $j = 2, 3, \ldots, n$.

Proof. Since $t_1 \in \mathbb{K}$ and $m_{1j} \in \mathbb{K}$ it follows that $t_j = t_1/m_{1j} \in \mathbb{K}$. Hence an easy induction applied to subsequent rows of the multiplicatively consistent matrix M finishes the proof of statement (a):

$$m_{ij} = \frac{m_{i-1,j}}{m_{i-1,i}} = \frac{t_{i-1}/t_j}{t_{i-1}/t_i} = \frac{t_i}{t_j}, \quad 1 < i, j \leq n.$$

Finally, Theorem 1 and (1) applied to (a) yields:

$$a_{ij} + s_j = \varphi(m_{ij}) + \varphi(t_j) = \varphi(t_i) = s_i,$$

where $a_{ij} = \varphi(m_{ij})$ and $s_j = \varphi(t_j)$.

Example 4. The canonical multiplicative and additive representations $[t_i/t_j]$ and $[s_i - s_j]$ of the consistent matrices M_1 and $A_1 = \log_{10}(M_1)$ (see Example 3) are congruent to:

$$M_1 = \begin{bmatrix} 1 & 4 & 11 \\ 5 & 1 & 17 \\ 7 & 9 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & \frac{1}{5} & \frac{1}{7} \\ \frac{5}{1} & 1 & \frac{5}{7} \\ \frac{7}{1} & \frac{7}{5} & 1 \end{bmatrix} \pmod{19}$$

and

$$A_1 = \begin{bmatrix} 0 & 16 & 6 \\ 2 & 0 & 8 \\ 12 & 10 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & -2 & -12 \\ 2 & 0 & -10 \\ 12 & 10 & 0 \end{bmatrix} \pmod{18}.$$

Indeed, if we take $t_1 = 1$ and $s_1 = 0$ then by Table 1 we obtain:

$$t_2 = t_1/m_{12} \equiv 5 \pmod{19}, \quad t_3 = t_1/m_{13} \equiv 7 \pmod{19},$$

$$s_2 = s_1 - a_{12} = -16 \equiv 2 \pmod{18}, \quad s_3 = s_1 - a_{13} \equiv 12 \pmod{18}.$$

Noticeably, both canonical representations of consistent matrices from $\mathcal{M}_n = \mathcal{M}_n(\mathbb{K})$ and $\mathcal{A}_n = \mathcal{A}_n(\mathbb{L})$ are useful in theory of the abstract consistent approximation. Similarly as in the classical case, one relies here on consistent projections $Q_n = Q_n^2$ of $\mathfrak{M}_{n\times n} \subset \mathbb{K}^{n\times n}$ onto $\mathcal{M}_n$ which are used in turn to approximate abstract PC matrices $M \in \mathfrak{M}_{n\times n}$ by their consistent images $Q_n(M)$. Now we introduce a new general concept of weighted consistent projections. In contrast to the classical case, we will not investigate the influence of positive weights $(\varrho_i)_{i=1}^n \in \mathbb{L}$ on topological properties of these projections. It should be noticed that the sum $\varrho_1 + \varrho_2 + \cdots + \varrho_n$ of weights may be equal to zero in the case, whenever $\mathbb{L}$ is a field of characteristic greater than 0.

Definition 2. Let φ be an homeomorphism between logarithmically homeomorphic groups $\mathbb{K}$ and $\mathbb{L}$. Let $(\varrho_i)_{i=1}^n$ be a vector of weights in $\mathbb{L} = \varphi(\mathbb{K})$ such that ϱ and ϱ_i/ϱ are not equal to zero. Then we define mapping $Q_n : \mathfrak{M}_{n\times n}(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ by the formula:

$$Q_n(M) = \varphi^{-1}(P_n(\varphi(M))) = [t_i/t_j], \quad M = [m_{ij}] \in \mathfrak{M}_{n\times n}(\mathbb{K}),$$

where $P_n : \mathfrak{A}_{n\times n}(\mathbb{L}) \to \mathcal{A}_n(\mathbb{L})$ is a mapping such that

$$P_n(\varphi(M)) = [s_i - s_j], \quad s_i = \sum_{j=1}^{n} \frac{\varrho_j}{\varrho}\varphi(m_{ij}) \quad \textit{and} \quad t_i = \varphi^{-1}(s_i).$$

The mappings Q_n and P_n are said to be *consistent*.

Lemma 2. *The consistent mappings Q_n and P_n are additive and multiplicative projections onto $\mathcal{A}_n(\mathbb{L})$ and $\mathcal{M}_n(\mathbb{K})$, respectively.*

Proof. If $X = [x_{ij}] \in \mathfrak{M}_{n\times n}(\mathbb{K})$ and $M = [m_{ij}] \in \mathfrak{M}_{n\times n}(\mathbb{K})$ then we can apply Definitions 2 and 1 to obtain:

$$\begin{aligned} Q_n(X \cdot M) &= \varphi^{-1}(P_n(\varphi(X \cdot M))) \\ &= \varphi^{-1}\left(\left[\sum_{k=1}^{n} \frac{\rho_k}{\varrho}(\varphi(x_{ik}m_{ik}) - \varphi(x_{jk}m_{jk}))\right]_{i,j=1}^{n}\right) \\ &= \varphi^{-1}(P_n(\varphi(X)) + P_n(\varphi(M))) = Q_n(X) \cdot Q_n(M), \end{aligned}$$

guaranteeing that Q_n is multiplicative projection and P_n is additive projection. Indeed, the latter follows from:

$$\begin{aligned} Q_n^2(M) &= Q_n\big[\varphi^{-1}(P_n(\varphi(M)))\big] = \varphi^{-1}[P_n(P_n(\varphi(M)))] \\ &= \varphi^{-1}\left(\left[\sum_{k=1}^{n} \frac{\varrho_k}{\varrho}(s_i - s_j)\right]_{i,j=1}^{n}\right) = \varphi^{-1}(P_n(\varphi(M))) = Q_n(M). \end{aligned}$$

The case of $\mathbb{K} = \mathbb{Z}_p^*$ and $\mathbb{L} = \mathbb{Z}_{p-1}$ coupled with Definition 2 and Lemma 2 leads to:

Theorem 2. *Let β be a generator of the multiplicative group $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ of positive remainders modulo a prime number p and let $\varphi(x) = \log_\beta x$ denote the discrete logarithm of $x \in \mathbb{Z}_p^*$ to the base β. If $(\varrho_i)_{i=1}^n$ are non-zero weights in $\mathbb{Z}_{p-1}$ such that $\sum_{i=1}^n \varrho_i \equiv 1 \,(mod\,(p-1))$, then ingredients $T = [t_i/t_j] \in \mathcal{M}_n$*

and $S = [s_i - s_j] \in \mathcal{A}_n$ *of the consistent projections* $P_n(\log_\beta M) = S$ *and* $Q_n(M) = T = \beta^S \in \mathcal{M}_n$ *satisfy the following formulae:*

$$s_i = \sum_{j=1}^{n} \varrho_j \log_\beta m_{ij} \in \mathbb{Z}_{p-1} \text{ and } t_i = \beta^{s_i} = \prod_{j=1}^{n} (m_{ij})^{\varrho_j} \in \mathbb{Z}_p^*,$$

for every matrix $M = [m_{ij}] \in \mathfrak{M}_{n\times n}$ *and* $i = 1, 2 \ldots, n$.

Proof. The first formula is a direct consequence of Definition 2 for $\varphi(x) = \log_\beta x$ and $\mathbb{K} = \mathbb{Z}_p^*$. Therefore, one can apply Remark 3 and (2) in order to obtain:

$$\beta^{s_i} = \beta^{\sum_{j=1}^{n} \log_\beta((m_{ij})^{\varrho_j})} = \prod_{j=1}^{n} (m_{ij})^{\varrho_j},$$

which in turn completes the proof.

Example 5. Suppose that $\mathbb{K} = \mathbb{Z}_{19}^*, \beta = 10$, $n = 3$, $\varrho_1 = \varrho_2 = \varrho_3 = 3^{-1} \equiv 13 \pmod{18}$ and

$$M = \begin{bmatrix} 1 & 11 & 12 \\ 5 & 1 & 9 \\ 8 & 17 & 1 \end{bmatrix}.$$

Visibly, it follows from the congruence $11 \cdot 9 \equiv 4 \pmod{19} \neq 12$ that the reciprocal matrix M is not multiplicatively consistent. Upon combining Theorem 2 with Table 1 and Table 2 one arrives at:

$$\begin{aligned} s_1 &= 13(\log_{10} 11 + \log_{10} 12) = 117 \equiv 9 \pmod{18}, \\ s_2 &= 13(\log_{10} 5 + \log_{10} 9) = 156 \equiv 12 \pmod{18}, \\ s_3 &= 13(\log_{10} 8 + \log_{10} 17) = 299 \equiv 11 \pmod{18}. \end{aligned}$$

Consequently as $s_1 - s_2 = -3 \equiv 15 \pmod{18}$, $s_1 - s_3 \equiv 16 \pmod{18}$ and $s_2 - s_3 \equiv 1 \pmod{18}$, the additive consistent projection $P_3(\log_\beta M)$ of M onto $\mathcal{A}_3$ is equal to:

$$S = \begin{bmatrix} 0 & 15 & 16 \\ 3 & 0 & 1 \\ 2 & 17 & 0 \end{bmatrix}.$$

In order to compute $t_i = 10^{s_i}$ one can use Table 1 to obtain $t_1 = 10^9 \equiv 10^{\log_{10} 18} \pmod{19} = 18$, and similarly $t_2 \equiv 7$ and $t_3 \equiv 14 \bmod 19$. Finally, with the aid of Table 2 one determines $t_1/t_2 = 18 \cdot 11 \equiv 8 \pmod{19}$, $t_1/t_3 \equiv 4 \pmod{19}$ and $t_2/t_3 \equiv 10 \pmod{19}$. Thus the multiplicative consistent projection $Q_3(M)$ of M onto $\mathcal{M}_3$ is equal to:

$$T = \begin{bmatrix} 1 & \frac{18}{7} & \frac{18}{14} \\ \frac{7}{18} & 1 & \frac{7}{14} \\ \frac{14}{18} & \frac{14}{7} & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 8 & 4 \\ 12 & 1 & 10 \\ 5 & 2 & 1 \end{bmatrix} \pmod{19}.$$

CONSISTENCY IN FINITE FIELDS $\mathbb{F}_{2^m}$, $m > 1$

The concept of consistent approximation can be generalized for all finite fields, extending the above setting derived to the fields $\mathbb{K} = \mathbb{Z}_p^*$ of remainders modulo a prime number p. In doing so, it is sufficient to establish formulae analogous to those presented in Theorem 2. Since each finite field is homeomorphic to a field $\mathbb{F}_{p^m}$ for some prime p and integer $m \geq 1$, we restrict our attention only to the most important in the computer design fields $\mathbb{F}_{2^m}$ of characteristic two, for which the multiplicative groups $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$ of order $N = 2^m - 1$ are cyclic. The general case of $p > 2$ and $m > 2$, can be treated in a similar, though slightly more complicated manner.

In order to introduce the mentioned above generalization, it is assumed that:

$$w_m(x) = x^m + \sum_{i=0}^{m-1} \omega_i x^i, \quad \omega_i \in \{0,1\},$$

is the primitive polynomial of degree m in the ring $\mathbb{Z}_2[x]$ of all polynomials of variable x with coefficients in the field $\mathbb{Z}_2$, which means that the following two conditions are satisfied:

1. $w_m(x)$ has no divisors in $\mathbb{Z}_2[x]$ of positive degrees;
2. $k = 2^m - 1$ is the smallest integer such that $w_m(x)$ divides $x^k - 1$.

Because of the importance of primitive polynomials $w_m(x)$ in applied cryptography, they are listed in the monograph [19] for every $m = 1, 2, \ldots, 229$. Moreover, if $2^m - 1$ is a Mersenne prime, then it is done for m less or equal to 44497. We notice that all primitive polynomials $w_m(x)$ over $\mathbb{Z}_2$ have the form similar to:

$$x^4 + x + 1, \quad x^7 + x + 1, \quad x^{31} + x^3 + 1, \quad x^{64} + x^4 + x^3 + x + 1.$$

The finite field $\mathbb{F}_{2^m} = (\mathbb{F}_{2^m}, +, \cdot)$ can then be represented as $\mathbb{Z}_2[x]/w_m(x)$ defining the set of all polynomials over $\mathbb{Z}_2$ modulo $w_m(x)$ with the polynomial $\beta = x$ forming a generator of $\mathbb{F}^*_{2^m}$. The sum $p(x) + q(x)$ of any two polynomials of degree at most $m - 1$,

$$p(x) = \sum_{i=0}^{m-1} a_i x^i \quad \text{and} \quad g(x) = \sum_{i=0}^{m-1} b_i x^i,$$

has the respective coefficients equal to $(a_i + b_i) \pmod 2$, while the product $p(x) \cdot g(x)$ is equal to a remainder of dividing the following polynomial

$$p(x)g(x) = \sum_{i=0}^{2m-2} \left(\left(\sum_{j=0}^{i} a_j b_{i-j} \right) \pmod 2 \right) x^i,$$

by $w_m(x)$. Here a_k and b_k are taken to be zero if $k < 0$ or $k \geq m$.

Taking into account the latter, one can identify the field $\mathbb{F}_{2^m}$ with the set of all binary numbers of the form:

$$a = (a_{m-1} \ldots a_0) = \sum_{i=0}^{m-1} a_i 2^i, \quad a_i \in \{0,1\},$$

under vector operations of addition and multiplication introduced above. Hence members of $\mathbb{F}_{2^m}$ have three different representations: a polynomial, a binary and a decimal one. For example, the standard generator $\beta = x$ of the cyclic group $\mathbb{F}^*_{2^m} = \mathbb{F}_{2^m} \setminus \{0\}$ and the primitive polynomial $w_m = w_m(x)$ can be represented as follows:

$$\beta = x = (\underbrace{0 \ldots 0}_{m-2} 10) = 2$$

and

$$w_m = x^m + \sum_{i=0}^{m-1} \omega_i x^i = (1 \omega_{m-1} \ldots \omega_0) = 2^m + \sum_{i=0}^{m-1} \omega_i 2^i.$$

Corollary 1. *It is convenient to represent the polynomials $w_m(x)$ and $p(x)$ in a computer as the binary numbers of length $2m$:*

$$w_m = (\underbrace{0 \ldots 01}_{m} \omega_{m-1} \ldots \omega_0), \quad a = (\underbrace{0 \ldots 0}_{m} a_{m-1} \ldots a_0).$$

Then coefficients of the product $p(x)q(x)$ can be determined by a fast algorithm based on the formula $F^{-1}(F(a) \cdot F(b))$, where $F \colon \mathbb{Z}_2^{2m} \to \mathbb{Z}_2^{2m}$ is the discrete Fourier transform and the multiplication $F(a) \cdot F(b)$ is understood coordinate-wise [18]. *In addition, the inverses and discrete logarithms of elements in $\mathbb{F}^*_{2^m} = \mathbb{F}_{2^m} \setminus \{0\}$ can be computed by the fast extended Euclidean and square-and-multiply polynomial algorithms* [19].

Example 6. The polynomial $w_4(x) = x^4 + x + 1$ is primitive over $\mathbb{Z}_2$. Hence the field $\mathbb{F}_{2^4} = \mathbb{Z}_2[x]/w_4(x)$ includes 15 polynomials of the form

$$\beta^k = a_3x^3 + a_2x^2 + a_1x + a_0, \quad k = 0, 1, \ldots, 14,$$

where $\beta = x$ is a generator in $\mathbb{F}^*_{2^4}$. Using the decimal notation of $\mathbb{F}_{2^4}$,

$$a = (a_3a_2a_1a_0) = 8a_3 + 4a_2 + 2a_1 + a_0 \in \mathbb{Z}_{15},$$

one can list the logarithms and inverses of these polynomials in Table 3.

Table 3. Discrete logarithms and inverses of elements $a \in \mathbb{F}^*_{2^4}$ with respect to the generator $\beta = x = (0010) = 2$.

$k = \log_\beta a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a = \beta^k$	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9
a^{-1}	1	9	13	15	14	7	10	5	11	12	6	3	8	4	2

In the next step a theorem on the weighted consistent approximation in the field $\mathbb{F}_q$ of order $q = 2^m$ is established and is illustrated by a carefully chosen example. For the simplicity the binary representations $a = (a_{m-1} \ldots a_0)$ of the members $p(x) = \sum_{i=0}^{m-1} a_i x^i$ of $\mathbb{F}_q$ are used. Moreover, we recall that matrices in $\mathcal{A}_n$ and $\mathcal{M}_n$ have now entries in the additive and multiplicative consistent groups $\mathbb{Z}_{q-1}$ and $\mathbb{F}^*_q$.

Theorem 3. *Let $\beta = x = (0 \ldots 010)$ be the generator of the group $\mathbb{F}^*_q$ for $q = 2^m$, and let $\varphi(a) = \log_\beta a$ denote the discrete logarithm of $a \in \mathbb{F}^*_q$ to the base β. If $(\varrho_i)_{i=1}^n$ are non-zero weights in $\mathbb{Z}_{q-1}$ such that*

$$\sum_{i=1}^{n} \varrho_i \equiv 1 \ (mod\,(q-1)),$$

then ingredients $T = [t_i/t_j]_{i,j=1}^n \in \mathcal{M}_n$ and $S = [s_i - s_j]_{i,j=1}^n \in \mathcal{A}_n$ of the consistent projections $P_n(\log_\beta M) = S$ and $Q_n(M) = T = \beta^S \in \mathcal{M}_n$ satisfy the following formulae:

$$s_i = \sum_{j=1}^{n} \varrho_j \log_\beta m_{ij} \in \mathbb{Z}_{q-1} \quad \text{and} \quad t_i = \beta^{s_i} = \prod_{j=1}^{n} (m_{ij})^{\varrho_j} \in \mathbb{F}^*_q,$$

for every PC matrix $M = [m_{ij}] \in \mathfrak{M}_{n\times n}$ with the entries in $\mathbb{F}^*_q$.

Proof. Since we have

$$\log_\beta(a \cdot b) = (\log_\beta a + \log_\beta b) \ (\mathrm{mod}\,(q-1))$$

and

$$\log_\beta(a^x) = x \log_\beta a \ (\mathrm{mod}\,(q-1)), \quad x \in \mathbb{Z}_{q-1},$$

we can set $\varphi(a) = \log_\beta a$ and $K_+ = \mathbb{F}^*_q$ in Definition 2 to derive the first formula. The latter directly yields the second formula, as we have:

$$\beta^{s_i} = \beta^{\sum_{j=1}^n \log_\beta((m_{ij})^{\varrho_j})} = \prod_{j=1}^{n} (m_{ij})^{\varrho_j},$$

which in turn combined with Lemma 2 completes the proof.

Example 7. Suppose that $q = 2^4$, $w_4(x) = x^4 + x + 1$ and $\mathbb{K} = \mathbb{F}_{2^4} = \mathbb{Z}_2[x]/w_4(x)$. In addition, consider the matrix $M \in \mathbb{K}^{3\times3}$ of the form:

$$M = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 1 \\ 9 & 1 & 1 \end{bmatrix}.$$

Since $x \cdot (x^3+1) \equiv 1 \pmod{w_4(x)}$ and $1 \cdot 1 \neq 2$ it follows that M is reciprocal, but not consistent. Take now $\varrho_1 = \varrho_3 = 4$, $\varrho_2 = 8$ in $\mathbb{Z}_{15}$ and determine the additive and multiplicative consistent projections:

$$P_3(\log_\beta M) = S = [s_i - s_j] \quad \text{and} \quad Q_3(M) = T = [t_i/t_j] = \beta^S.$$

For this purpose, we apply Theorem 2 and Table 3 in order to obtain:

$$s_1 = 4\log_\beta 2 \equiv 4 \pmod{15}, \quad s_2 = 0, \quad s_3 = 4\log_\beta 9 = 96 \equiv 1 \pmod{15},$$

$$s_1 - s_2 = 4, \quad s_1 - s_3 = 3, \quad s_2 - s_3 = -1 \equiv 14 \pmod{15}.$$

Moreover, with the aid of decimal notation one concludes that polynomials $t_i = \beta^{s_i}$, $t_i/t_j \in \mathbb{F}_{2^4}^*$ are equal to:

$$t_1 = \beta^4 = 3, \quad t_2 = \beta^0 = 1, \quad t_3 = \beta^1 = 2, \quad t_1/t_2 = 3,$$

$$t_1/t_3 = 3 \cdot 2^{-1} = 3 \cdot 9 = 7, \quad t_2/t_3 = 2^{-1} = 9,$$

where product $3 \cdot 9 = (0011) \cdot (1001)$ are computed according to:

$$(x+1)(x^3+x) \equiv (x^3+x^2+1) \pmod{w_4(x)} = (0111) = 7.$$

Finally, consistent projections of the matrix M are equal to:

$$P_3(\log_\beta M) = \begin{bmatrix} 0 & 4 & 3 \\ 11 & 0 & 14 \\ 12 & 1 & 0 \end{bmatrix}$$

and

$$Q_3(M) = \begin{bmatrix} 1 & \frac{3}{1} & \frac{3}{2} \\ \frac{1}{3} & 1 & \frac{1}{2} \\ \frac{2}{3} & \frac{2}{1} & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 & 7 \\ 14 & 1 & 9 \\ 6 & 2 & 1 \end{bmatrix} \pmod{w_4(x)}.$$

AN EXTENTION OF CONSISTENT PROJECTION

In Abstract Consistent Projections section the consistent projections $Q_n \colon \mathfrak{M}_{n\times n}(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ for all reciprocal matrices with entries in $\mathbb{K}$ are defined. It is of considerable interest and particular importance that their range $\mathfrak{M}_{n\times n}(\mathbb{K})$ can be extended to the set of all $\mathbb{K}$ – valued matrices, at least when $\mathbb{K} = \mathbb{F}_q^*$ with $q = 2^m$. For this purpose, let $\beta = x = (0\ldots010)$ and $\mathfrak{K}_{n\times n}(\mathbb{K})$ denote the generator of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and the set of all matrices $M = [m_{ij}]$ with entries in $\mathbb{F}_q^*$, respectively. Moreover, suppose that $(\varrho_i)_{i=1}^n$ are non-zero weights in $\mathbb{Z}_{q-1}$ such that:

$$\sum_{i=1}^{n} \varrho_i \equiv 1 \pmod{(q-1)}.$$

Theorem 4. *Let $\hat{Q}_n \colon \mathfrak{K}_{n\times n}(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ be a consistent mapping defined by the following formula:*

$$\hat{Q}_n(M) = \beta^{P_n(\log_\beta \sqrt{\hat{M}})} = [t_i/t_j],$$

where $M = [m_{ij}]$, $\hat{M} = \left[\frac{m_{ij}}{m_{ji}}\right]$, $P_n(\log_\beta \sqrt{\hat{M}}) = [s_i - s_j]$, $t_i = \beta^{s_i}$ and

$$s_i = 2^{m-1} \sum_{j=1}^{n} \varrho_j \log_\beta \frac{m_{ij}}{m_{ji}}, \quad i = 1, 2, \ldots, n.$$

Then $\hat{Q}_n = \hat{Q}_n^2$ is an extension of the consistent projection $Q_n \colon \mathfrak{M}_{n\times n}(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$ to the range $\mathfrak{K}_{n\times n}(\mathbb{K})$.

Proof. Observe that each element $a \in \mathbb{F}_{2^m}$ has exactly one square root, namely $\sqrt{a} = a^{2^{m-1}}$. Consequently, by Remark 3 we arrive at:

$$\log_\beta \sqrt{\hat{M}} = 2^{m-1}\left[\log_\beta \frac{m_{ij}}{m_{ji}}\right]_{i,j=1}^{n} \quad \text{and} \quad \sqrt{\frac{m_{ij}}{m_{ji}}}\sqrt{\frac{m_{ji}}{m_{ij}}} = 1.$$

Thus one can apply Theorem 3 to the reciprocal matrix $\sqrt{\hat{M}}$ in order to obtain the formulae for t_i and s_i. Furthermore, if $M = [m_{ij}] \in \mathfrak{M}_{n\times n}$, then conditions $m_{ij}m_{ji} = 1$ of reciprocity and Fermat's theorem yield:

$$\sqrt{\hat{M}} = [\sqrt{m_{ij}^2}] = [m_{ij}^{2^m}] = [m_{ij}] = M,$$

which renders $\hat{Q}_n(M) = Q_n(M) = M$ on $\mathfrak{M}_{n\times n}(\mathbb{K})$. Since each matrix $T = [t_i/t_j]$ is consistent, it follows that:

$$\hat{Q}_n^2(M) = \hat{Q}_n(T) = Q_n(T) = T = \hat{Q}_n(M),$$

for every $M \in \mathfrak{K}_{n\times n}(\mathbb{K})$. Hence $\hat{Q}_n$ is a projection.

THE CASE OF ONE PARAMETER GROUPS

In this section we focus our attention on an extension of pairwise comparisons to the algebra $\mathcal{B}(H)$ of all bounded linear operators from a complex Hilbert space H into H. For this purpose we recall that an operator $A \in \mathcal{B}(H)$ is said to be positive if the following inner products satisfy

$$\langle Ah, h\rangle \geq 0, \text{ for all } h \in H.$$

The positivity of A is denoted by $A \geq 0$. The notion of positivity enables to make the algebra $\mathcal{B}(H)$ as well the algebra $\mathfrak{RB}(H)$ of hermitian operators on H into ordered vector spaces in the usual way [17].

Furthermore, we recall that a function $U : \mathbb{R} \to \mathcal{B}(H)$ is said to be a (strongly) continuous one-parameter unitary group if for all α and β in $\mathbb{R}$ we have:

(a) $U(\alpha)$ is a unitary operator,

(b) $U(\alpha + \beta) = U(\alpha)U(\beta)$,

(c) if $h \in H$, then $U(\alpha)h \to U(\beta)h$ as $\alpha \to \beta$.

By the Stone's Theorem (see [17]) the function U is a continuous one parameter unitary group if and only if there is a self-adjoint operator A such that

$$U(\alpha) = \exp(i\alpha A) \quad \text{or} \quad i\alpha A = \log U(\alpha), \quad \alpha \in \mathbb{R}.$$

This self-adjoint operator A is said to be infinitesimal operator of U. It may be unbounded and

$$Ah = \lim_{\alpha\to 0} \frac{U(\alpha)h - h}{\alpha}, \quad h \in dom(A),$$

where linear manifold $dom(A)$ is dense in H. It consists of all vectors h in H such that the limit exists. Moreover, the operator $i\alpha A$ is antisymmetric for every α in $\mathbb{R}$. Indeed, if $f, g \in dom(A)$, then we have

$$\langle i\alpha Af, g\rangle = i\alpha \langle f, Ag\rangle = -\langle f, i\alpha Ag\rangle .$$

Note that the subset $\mathbb{K}$ of $\mathcal{B}(H)$ defined by

$$\mathbb{K} = U(\mathbb{R}) = \{U(\alpha) : \alpha \in \mathbb{R}\} = \{\exp(i\alpha A) : \alpha \in \mathbb{R}\}$$

is a multiplicative group with the identity and inverse equal to:

$$U(0) = 1 \quad \text{and} \quad U(-\alpha) = U(\alpha)^{-1}.$$

Hence one can apply our results from previous sections and derive formulae for multiplicative consistent projections of a reciprocal matrix $M = [m_{ij}]_{n\times n}$ with entries in a one parameter unitary group $\mathbb{K}$ onto the group $\mathcal{M}_n(\mathbb{K})$ of all multiplicatively consistent matrices $T = [t_{kj}]_{n\times n}$ with entries in $\mathbb{K} = U(\mathbb{R})$:

$$t_{kj} = U(\alpha_{kj}), \quad k, j = 1, 2, \ldots, n.$$

For this purpose, we have to construct first an auxiliary additive consistent projection of the antisymmetric matrix $\log M = [\log m_{kj}]_{n\times n}$ onto the group $\mathcal{A}_n(\mathbb{L})$ of all additively consistent matrices $\mathcal{S} = [s_{kj}]_{n\times n}$ with entries $\mathbb{L} = \log U(\mathbb{R})$:

$$s_{kj} = \log U(\alpha_{kj}) = i\alpha_{kj}A, \quad k, j = 1, 2, \ldots, n.$$

In the following theorem, each composition

$$U(\alpha)U(\beta)^{-1} = U(\alpha)U(-\beta)$$

of operators in $\mathbb{K} = U(\mathbb{R})$ will be written as a ratio $U(\alpha)/U(\beta)$.

Theorem 5. *Let the multiplicative group $\mathbb{K} = U(\mathbb{R})$ be the range of a continuous one-parameter unitary group $U : \mathbb{R} \to \mathcal{B}(H)$ such that $U(\alpha) = \exp(i\alpha A)$ for every real α, and let the additive group $\mathbb{L}$ be defined by*

$$\mathbb{L} = \log U(\mathbb{R}) = \{i\alpha A : \alpha \in \mathbb{R}\},$$

where A is infinitesimal generator of U. If $(\rho_i)_{i=1}^n$ are positive weights such that $\sum_{i=1}^n \rho_i = 1$, then ingredients of the consistent projections

$$Q_n(M) = [t_k/t_j] \in \mathcal{M}_n(\mathbb{K}) \quad \text{and} \quad P_n(\log M) = [s_k - s_j] \in \mathcal{A}_n(\mathbb{L})$$

satisfy the formulae

$$t_k = \exp s_k \quad \text{and} \quad s_k = \sum_{j=1}^{n} \rho_j \log U(\alpha_{kj}) = iA \sum_{j=1}^{n} \rho_j \alpha_{kj},$$

for every reciprocal matrix M of the form

$$M = [m_{kj}] = [U(\alpha_{kj})] \in \mathfrak{M}_{n\times n}(\mathbb{K}).$$

Proof. As in the proof of Theorem 2 we apply Definition 2 and Lemma 2 with the abstract logarithm defined by

$$\varphi(M) = \log M = [i\alpha_{kj}A]_{n\times n}.$$

CONCLUSIONS

A study of groups permitting an effective and unified design of weighted projections of abstract reciprocal matrices onto consistent matrices is addressed within the theory of pairwise comparisons. It is shown that this is possible for pairs of multiplicative and additive groups, which are mutually logarithmically homeomorphic. It means that the group of multiplicative type is mapped onto the group of additive type by an abstract logarithm function.

In this paper we have focused our attention mainly on consistent additive and multiplicative projections not only for the discrete modular groups $\mathbb{Z}_p^*$ and $\mathbb{F}_{2^m}^*$ but also for one parameter unitary groups in the algebra of all bounded linear operators from a Hilbert space into itself. It has been partially motivated by several applications of these groups in computer sciences, applied mathematics, cryptography and others. By the same reasons it would be of interest to develop pairwise comparisons in other classes of groups, in particular elliptic groups, i.e., groups of rational points on elliptic curves. Finally, we note that another important motivation of study of pairwise comparisons in an abstract setting comes from the field of computer science priority theory.

REFERENCES

[1] Saaty TL. The Analytic Hierarchy Process. New York: McGraw Hill; 1980.

[2] Saaty TL. A scaling method for priorities in hierarchical structure. Journal of Mathematical Psychology. 1997;15:234–281.

[3] van Laarhoven PJM, Pedrycz W. A fuzzy extension of Saaty's priority theory. Fuzzy Sets and Systems. 2018;11:229–241.

[4] Koczkodaj WW, Orłowski M. An orthogonal basis for computing a consistent approximation to a pairwise comparisons matrix. Computers and Mathematics with Applications. 1997;34:41–47.

[5] Cavallo B, Brunelli M. A general unified framework for interval pairwise comparisons matrices. International Journal of Approximate Reasoning. 178–198;93:2018.

[6] Farkas A, Lancaster P, Rozsa P. Approximation of positive matrices by transitive matrices. Computers and Mathematics with Applications. 2005;50:1033–1039.

[7] Koczkodaj WW, Szarek SJ. On distance-based consistency reduction algorithms for pairwise comparisons. Logic Journal of the IGPL. 2010;18:859–869.

[8] Holsztyński W, Koczkodaj WW. Convergence of inconsistency algorithms for the pairwise comparisons. Information Processing Letters. 1996;59:197–202.

[9] Koczkodaj WW, Szwarc R. On axiomatization of inconsistency indicators for pairwise comparisons. Fundamenta Informaticae. 2014;132:485–500.

[10] Koczkodaj WW, Smarzewski R, Szybowski J. On orthogonal projections on the space of consistent pairwise comparisons matrices. Fundamenta Informaticae. 2020;172:379–397.

[11] Smarzewski R, Rutka P. Consistent projections and indicators in pairwise comparisons. International Journal of Approximate Reasoning. 2020;124:123–132.

[12] Kendall MG, Babington-Smith B. On the method of paired comparisons. Biometrika. 1940;31:324–345.

[13] Wajch E. From pairwise comparisons to consistency with respect to a group operation and Koczkodaj's metric. International Journal of Approximate Reasoning. 2019;106:51–62.

[14] Koczkodaj WW, Liu F, Marek VW, Mazurek J, Mazurek M, Mikhailov L, et al. On the use of group theory to generalize elements of pairwise comparisons matrix: a cautionary note. International Journal of Approximate Reasoning. 2020;124:59–65.

[15] Durnoga K, Pomykała J. Large sieve, Miller-Rabin compositeness witnesses and integer factoring problem. Fundamenta Informaticae. 2017;156:179–185.

[16] Durnoga K, Źrałek B. On computing discrete logarithms and bulk and randomness extractors. Fundamenta Informaticae. 2015;141:345–366.

[17] Conway JB. A Course in Functional Analysis. Berlin: Springer; 1990.

[18] Aho AV, Hopcroft JE, Ullman JD. The Design and Analysis of Computer Algorithms. London: Addison-Wesley; 1974.

[19] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. New York: CRC; 1997.

[20] Husemöller D. Elliptic Curves. New York: Springer-Verlag; 2004.

[21] Washington LC. Elliptic Curves Number Theory and Cryptography. New York: CRC; 2008.