Computer Science Journal of Moldova, vol.**30**, no.2(89), 2022

On Elimination of Erasing Rules from E0S Grammars

Alexander Meduna, Martin Havel

Abstract

The present paper describes an alternative algorithm for the removal of erasing rules from E0S grammars. As opposed to the standard way of eliminating erasing rules in most E0S-like grammars, such as context-free grammars, this method requires no predetermination of symbols that derive the empty string. The proposed algorithm is formally verified. In the conclusion of the paper, the applicability of the algorithm to E0S grammars that work in a semi-parallel way is demonstrated. Furthermore, two open problems are formulated.

Keywords: Formal languages, E0S grammars, elimination of erasing rules.

MSC 2020: 68Q45, 03D05, 68Q70.

1 Introduction

In the theory of formal languages, E0S grammars represent, in essence, ordinary context-free grammars generalized so they can rewrite both terminal and nonterminal symbols. Recall that these grammars underlie some important general frameworks of context-free rewriting systems, such as selective substitution grammars (see [2] and [3]).

The standard method of eliminating erasing rules from E0S grammars and their special cases, such as context-free grammars, requires a predetermination of symbols that derive the empty string (see, for instance, Section 5.1.3.2 in [9]). Of course, the theory of formal languages would highly appreciate obtaining an alternative method that performs this elimination without any predetermination like this. The present paper achieves such a method. Indeed, it presents and verifies an alternative algorithm that performs

©2022 by CSJM; A. Meduna, M. Havel
doi:10.56415/csjm.v30.08

the elimination of erasing rules from E0S grammars without this predetermination. In addition, it is demonstrated that this algorithm is straightforwardly applicable to E0S grammars working in a semi-parallel way, too. Several other derivation modes are also discussed.

The paper is organized as follows. First, Section 2 gives all the necessary terminology. Then, Section 3 presents the main result of the paper—that is, it describes and verifies an alternative algorithm for the elimination of erasing rules from E0S grammars. Finally, Section 4 discusses the applicability of our algorithm to other derivation modes used in E0S grammars, and formulates two open problems.

2 Preliminaries and Definitions

This paper assumes that the reader is familiar with formal language theory (see [11]). For an alphabet (finite nonempty set) V, V^* represents the free monoid generated by V. The unit of V^* is denoted by ε. Set $V^+ = V^* - \{\varepsilon\}$; algebraically, V^+ is thus the free semigroup generated by V. For $w \in V^*$, $|w|$ denotes the length of w, and $\mathrm{alph}(w)$ denotes the set of symbols occurring in w. As usual, we consider two languages L_1, L_2 to be equal if and only if $L_1 - \{\varepsilon\} = L_2 - \{\varepsilon\}$, and we simply write $L_1 = L_2$ in this case. The inclusion relation of languages is interpreted similarly.

An *E0S grammar* (see [2] and [3]) is a quadruple, $G = (V, T, P, S)$, where V is an alphabet, $T \subset V$, $S \in V - T$, and $P \subseteq V \times V^*$ is a finite relation. The components V, T, P, and S are called the *total alphabet*, the alphabet of *terminal symbols*, the set of *rules*, and the *start symbol*, respectively. Each $(X, y) \in P$ is written as $X \to y$ throughout this paper. G is said to be *propagating* if and only if every $X \to y \in P$ satisfies $y \in V^+$. Rules of the form $X \to \varepsilon$ are called *erasing rules*. The *direct derivation relation* over V^*, denoted by $\Rightarrow_G$, is defined as follows: $uXv \Rightarrow_G uyv$ if and only if $X \to y \in P$ and $u, v \in V^*$. Let $\Rightarrow_G^n$ and $\Rightarrow_G^*$ denote the nth power of $\Rightarrow_G$, for some $n \geq 0$, and the reflexive-transitive closure of $\Rightarrow_G$, respectively. The *language of* G is denoted by $L(G)$ and defined as $L(G) = \{w \in T^* \mid S \Rightarrow_G^* w\}$. Observe that the language family generated by E0S grammars coincides with the family of context-free languages.

Let $G = (V, T, P, S)$ be an E0S grammar. For any $X \Rightarrow_G^* y$, where $X \in V$ and $y \in V^*$, $\Delta(X \Rightarrow_G^* y)$ denotes its corresponding derivation tree. Regarding

derivation trees and related notions, we use the terminology of Section 5.1.1 in [9]. We straightforwardly extend these notions from context-free grammars to E0S grammars. A derivation subtree whose frontier is ε is called an ε-*subtree*. Let $S \Rightarrow_G^* w$ be of the form $S \Rightarrow_G^* yxz \Rightarrow_G^* w$, where $x, y, z \in V^*$ and $w \in T^*$. We write $S \Rightarrow_G^* y\,{}^{\varepsilon}x\,z \Rightarrow_G^* w$ to express that either (1) $x = \varepsilon$ or (2) all subtrees in $\Delta(S \Rightarrow_G^* w)$ rooted at the symbols in x are ε-subtrees; informally, it means that x is erased in the rest of the derivation.

3 Main Result

In this section, we present and verify an alternative algorithm that performs the elimination of erasing rules from E0S grammars. To give a more detailed insight into this algorithm, consider an arbitrary E0S grammar, $G = (V, T, P, S)$, and $Y \in V$. If Y derives ε in G, then a derivation like this can be expressed in the following step-by-step way:

$$Y \Rightarrow_G y_1 \Rightarrow_G y_2 \Rightarrow_G \cdots \Rightarrow_G y_n \Rightarrow_G \varepsilon,$$

where $y_i \in V^*$ for all $i = 1, \ldots, n$, for some $n \geq 1$. If a sentential form contains several occurrences of Y, each of them can be erased in this way although there may exist many alternative ways of erasing Y. Based upon these observations, the next algorithm introduces compound nonterminals of the form $\langle X, U \rangle$, in which X is a symbol that is not erased during the derivation, and U is a set of symbols that are erased. Within the compound nonterminal, the algorithm simulates the erasure of symbols in U in the way sketched above. Observe that since U is a set, U contains no more than one occurrence of any symbol because there is no need to record several occurrences of the same symbol; indeed, as already pointed out, all these occurrences can be erased in the same way.

Algorithm 1. *An alternative elimination of erasing rules in E0S grammars without any predetermination of symbols that derive the empty string.*

Input: An E0S grammar, $G = (V, T, P, S)$.

Output: A propagating E0S grammar, $H = (V', T, P', S')$, such that $L(G) = L(H)$.

Method: Initially, set $V' = T \cup \{\langle X,U\rangle \mid X \in V, U \subseteq V\}$, $S' = \langle S,\emptyset\rangle$, and

$$P' = \{\langle a,\emptyset\rangle \to a \mid a \in T\}.$$

Repeat (1) and (2), given next, until P' cannot be extended.

(1) **If** $Y \to y_0Y_1y_1Y_2y_2\cdots Y_ny_n \in P$, where $y_i \in V^*$, $Y_j \in V$, for all i and j, $0 \le i \le n$, $1 \le j \le n$, for some $n \ge 1$,
then for every $U \subseteq V$, extend P' by adding

$$\langle Y,U\rangle \to \langle Y_1, U \cup \mathrm{alph}(y_0y_1\cdots y_n)\rangle\langle Y_2,\emptyset\rangle\cdots\langle Y_n,\emptyset\rangle.$$

(2) **If** $\langle X,U\rangle \in V'$ and $Y \to y \in P$, where $Y \in U$ and $y \in V^*$,
then extend P' by adding

$$\langle X,U\rangle \to \langle X, (U - \{Y\}) \cup \mathrm{alph}(y)\rangle. \qquad \square$$

Let us point out that the algorithm makes no predetermination of symbols from which ε can be derived as opposed to most standard methods of removing erasing rules, including the standard removal of erasing rules from context-free grammars (see, for instance, Section 5.1.3.2 in [9]). Indeed, if the output grammar improperly extends the second component of a two-component nonterminal by a symbol that is not erased throughout the rest of the derivation, then this occurrence of the symbol never disappears in this component, so a terminal string cannot be generated under this improper selection. It is also worth pointing out that the cardinality of V' and P' exponentially increases with respect to the cardinality of V and P, respectively.

Before we verify the correctness of the presented algorithm, we illustrate it by an example.

Example 1. Consider the E0S grammar

$$G = \big(\{S,a,b\},\{a,b\},\{S \to aSb, S \to \varepsilon\},S\big).$$

Clearly, $L(G) = \{a^nb^n \mid n \ge 0\}$. With G as its input, Algorithm 1 produces a propagating E0S grammar H whose fully detailed definition is left to the reader. We only describe the derivations of *aabb* in G and in H. That is,

$$S \Rightarrow_G aSb \Rightarrow_G aaSbb \Rightarrow_G aabb$$

and

$$\langle S,\emptyset\rangle \Rightarrow_H \langle a,\emptyset\rangle\langle S,\emptyset\rangle\langle b,\emptyset\rangle \Rightarrow_H \langle a,\emptyset\rangle\langle a,\{S\}\rangle\langle b,\emptyset\rangle\langle b,\emptyset\rangle$$

$$\Rightarrow_H \langle a,\emptyset\rangle\langle a,\emptyset\rangle\langle b,\emptyset\rangle\langle b,\emptyset\rangle \Rightarrow_H^4 aabb. \qquad \square$$

We proceed to a formal verification of Algorithm 1.

Theorem 1. Let G be an E0S grammar. Algorithm 1 halts and correctly converts G to a propagating E0S grammar H satisfying $L(G) = L(H)$.

Proof. Clearly, the algorithm always halts. Since P' does not contain any erasing rules, H is propagating. To establish $L(H) = L(G)$, we prove three claims.

The first claim shows how derivations of G are simulated by H. It is used to prove that $L(G) \subseteq L(H)$ later in the proof. Recall that the meaning of ${}^{\varepsilon}x$ is defined in Section 2.

Claim 1. *If* $S \Rightarrow_G^m {}^{\varepsilon}x_0X_1{}^{\varepsilon}x_1X_2{}^{\varepsilon}x_2\cdots X_h{}^{\varepsilon}x_h \Rightarrow_G^* z$, *where* $z \in L(G)$, $|z| \geq 1$, $x_i \in V^*$, $X_j \in V$, *for all* i *and* j, $0 \leq i \leq h$, $1 \leq j \leq h$, *for some* $m \geq 0$ *and* $h \geq 1$, *then* $\langle S,\emptyset\rangle \Rightarrow_H^* \langle X_1,U_1\rangle\langle X_2,U_2\rangle\cdots\langle X_h,U_h\rangle$, *where* $\bigcup_{1\leq i\leq h} U_i \subseteq \bigcup_{0\leq i\leq h} \mathrm{alph}(x_i)$.

Proof. This claim is established by induction on $m \geq 0$.

Basis. The basis for $m = 0$ is clear.

Induction Hypothesis. Suppose that the claim holds for all derivations of length ℓ, where $0 \leq \ell \leq m$, for some $m \geq 0$.

Induction Step. Consider any derivation of the form

$$S \Rightarrow_G^{m+1} w \Rightarrow_G^* z,$$

where $w \in V^+$, $z \in L(G)$, and $|z| \geq 1$. Since $m+1 \geq 1$, this derivation can be expressed as

$$S \Rightarrow_G^m x \Rightarrow_G w \Rightarrow_G^* z,$$

where $x \in V^+$. Let $x = {}^{\varepsilon}x_0X_1{}^{\varepsilon}x_1X_2{}^{\varepsilon}x_2\cdots X_h{}^{\varepsilon}x_h$, where $x_i \in V^*$, $X_j \in V$, for all i and j, $0 \leq i \leq h$, $1 \leq j \leq h$, for some $h \geq 1$. Then, by the induction hypothesis,

$$\langle S,\emptyset\rangle \Rightarrow_H^* \langle X_1,U_1\rangle\langle X_2,U_2\rangle\cdots\langle X_h,U_h\rangle,$$

where $\bigcup_{1\leq i\leq h} U_i \subseteq \bigcup_{0\leq i\leq h} \text{alph}(x_i)$, for some $n \geq 0$.

Next, we consider all possible forms of $x \Rightarrow_G w$, covered by the next two cases—(i) and (ii).

(i) Let $X_j \to y_0 Y_1 y_1 \cdots Y_q y_q \in P$, where $y_i \in V^*$, for all i, $0 \leq i \leq q$, $Y_i \in V$, for all i, $1 \leq i \leq q$, for some j, $1 \leq j \leq h$, and $q \geq 1$, so

$$\begin{gathered}{}^{\varepsilon}x_0 X_1 {}^{\varepsilon}x_1 \cdots X_j {}^{\varepsilon}x_j \cdots X_h {}^{\varepsilon}x_h \Rightarrow_G \\ {}^{\varepsilon}x_0 X_1 {}^{\varepsilon}x_1 \cdots X_{j-1} {}^{\varepsilon}x_{j-1} {}^{\varepsilon}y_0 Y_1 {}^{\varepsilon}y_1 \cdots Y_q {}^{\varepsilon}y_q {}^{\varepsilon}x_j X_{j+1} {}^{\varepsilon}x_{j+1} \cdots X_h {}^{\varepsilon}x_h.\end{gathered}$$

By (1) in the algorithm,

$$\langle X_j, U_j\rangle \to \langle Y_1, U_j \cup \text{alph}(y_0 y_1 \cdots y_q)\rangle \langle Y_2, \emptyset\rangle \cdots \langle Y_q, \emptyset\rangle \in P'$$

so

$$\begin{gathered}\langle X_1, U_1\rangle \langle X_2, U_2\rangle \cdots \langle X_j, U_j\rangle \cdots \langle X_h, U_h\rangle \Rightarrow_H \\ \langle X_1, U_1\rangle \langle X_2, U_2\rangle \cdots \langle X_{j-1}, U_{j-1}\rangle \langle Y_1, U_j \cup \text{alph}(y_0 y_1 \cdots y_q)\rangle \\ \langle Y_2, \emptyset\rangle \cdots \langle Y_q, \emptyset\rangle \langle X_{j+1}, U_{j+1}\rangle \cdots \langle X_h, U_h\rangle.\end{gathered}$$

Clearly,

$$\begin{gathered}\left(\bigcup_{1\leq i\leq h} U_i\right) \cup \left(\bigcup_{0\leq i\leq q} \text{alph}(y_i)\right) \subseteq \\ \left(\bigcup_{0\leq i\leq h} \text{alph}(x_i)\right) \cup \left(\bigcup_{0\leq i\leq q} \text{alph}(y_i)\right)\end{gathered}$$

which completes the induction step for (i).

(ii) Let $x_j = x'_j Y x''_j$ and $Y \to y \in P$, where $y \in V^*$ and $x'_j, x''_j \in V^*$, so

$${}^{\varepsilon}x_0 X_1 {}^{\varepsilon}x_1 \cdots X_j {}^{\varepsilon}x_j \cdots X_h {}^{\varepsilon}x_h \Rightarrow_G {}^{\varepsilon}x_0 X_1 {}^{\varepsilon}x_1 \cdots X_j {}^{\varepsilon}x'_j {}^{\varepsilon}y {}^{\varepsilon}x''_j \cdots X_h {}^{\varepsilon}x_h.$$

If $Y \notin \bigcup_{1\leq i\leq h} U_i$, then

$$\langle X_1, U_1\rangle \langle X_2, U_2\rangle \cdots \langle X_h, U_h\rangle \Rightarrow_H^0 \langle X_1, U_1\rangle \langle X_2, U_2\rangle \cdots \langle X_h, U_h\rangle$$

and clearly

$$\bigcup_{1\leq i\leq h} U_i \subseteq \left(\bigcup_{0\leq i\leq h, i\neq j} \text{alph}(x_i)\right) \cup \text{alph}\left(x'_j y x''_j\right)$$

so assume that $Y \in \bigcup_{1\leq i\leq h} U_i$. By (2) in the algorithm,

$$\langle X_k, U_k\rangle \to \langle X_k, (U_k - \{Y\}) \cup \mathrm{alph}(y)\rangle \in P',$$

where $U_k = U'_k \cup \{Y\}$, $U'_k \subseteq V$, for some k, $1 \leq k \leq h$, so

$$\langle X_1, U_1\rangle\langle X_2, U_2\rangle \cdots \langle X_k, U_k\rangle \cdots \langle X_h, U_h\rangle \Rightarrow_H$$
$$\langle X_1, U_1\rangle\langle X_2, U_2\rangle \cdots \langle X_k, (U_k - \{Y\}) \cup \mathrm{alph}(y)\rangle \cdots \langle X_h, U_h\rangle.$$

Clearly,

$$\left(\bigcup_{1\leq i\leq h, i\neq k} U_i\right) \cup \left(U'_k \cup \mathrm{alph}(y)\right) \subseteq \left(\bigcup_{0\leq i\leq h, i\neq j} \mathrm{alph}(x_i)\right) \cup \mathrm{alph}\left(x'_j y x''_j\right)$$

which completes the induction step for (ii).

Observe that these two cases cover all possible derivations of the form $x \Rightarrow_G w$. Thus, the claim holds. □

The second claim shows that in H, every derivation of any $z \in L(H)$ can be expressed as a two-part derivation. In the first part, every occurring symbol is a two-component nonterminal. In the second part, only the rules of the form $\langle a, \emptyset\rangle \to a$, where $a \in T$, are used.

Claim 2. *For every $z \in L(H)$, there exists a derivation $\langle S, \emptyset\rangle \Rightarrow_H^* x \Rightarrow_H^* z$, where $x \in V'^+$, and during $x \Rightarrow_H^* z$, only rules of the form $\langle a, \emptyset\rangle \to a$, where $a \in T$, are used.*

Proof. Since H is an E0S grammar, we can always rearrange all the applications of rules so the claim holds. □

The third claim shows how derivations of H are simulated by G. It is used to prove that $L(H) \subseteq L(G)$ later in the proof.

Claim 3. *If $\langle S, \emptyset\rangle \Rightarrow_H^n \langle X_1, U_1\rangle\langle X_2, U_2\rangle \cdots \langle X_h, U_h\rangle$, where $X_i \in V$ and $U_i \subseteq V$, for all i, $1 \leq i \leq h$, for some $n \geq 0$ and $h \geq 1$, then $S \Rightarrow_G^* x_0 X_1 x_1 X_2 x_2 \cdots X_h x_h$, where $x_i \in V^*$, for all i, $0 \leq i \leq h$, and $\bigcup_{1\leq i\leq h} U_i \subseteq \bigcup_{0\leq i\leq h} \mathrm{alph}(x_i)$.*

Proof. This claim is established by induction on $n \geq 0$.

Basis. The basis for $n = 0$ is clear.

Induction Hypothesis. Suppose that the claim holds for all derivations of length ℓ, where $0 \leq \ell \leq n$, for some $n \geq 0$.

Induction Step. Consider any derivation of the form

$$\langle S, \emptyset \rangle \Rightarrow_H^{n+1} w,$$

where $w \in V'^+$. Since $n+1 \geq 1$, this derivation can be expressed as

$$\langle S, \emptyset \rangle \Rightarrow_H^{n} x \Rightarrow_H w,$$

where $x \in V'^+$. Let $x = \langle X_1, U_1 \rangle \langle X_2, U_2 \rangle \cdots \langle X_h, U_h \rangle$, where $X_i \in V$, $U_i \in V^*$, for all i, $1 \leq i \leq h$, for some $h \geq 1$. By the induction hypothesis,

$$S \Rightarrow_G^* x_0 X_1 x_1 X_2 x_2 \cdots X_h x_h,$$

where $x_i \in V^*$, for all i, $1 \leq i \leq h$, such that $\bigcup_{1 \leq i \leq h} U_i \subseteq \bigcup_{0 \leq i \leq h} \text{alph}(x_i)$.

Next, we consider all possible forms of $x \Rightarrow_H w$, covered by the next two cases—(i) and (ii).

(i) Let $\langle X_j, U_j \rangle \to \langle Y_1, W \rangle \langle Y_2, \emptyset \rangle \cdots \langle Y_q, \emptyset \rangle \in P'$ be a rule introduced in (1) in the algorithm, where $W \subseteq V$ and $Y_i \in V$, for all i, $1 \leq i \leq q$, for some $q \geq 1$, so

$$\langle X_1, U_1 \rangle \langle X_2, U_2 \rangle \cdots \langle X_j, U_j \rangle \cdots \langle X_h, U_h \rangle \Rightarrow_H$$
$$\langle X_1, U_1 \rangle \cdots \langle X_{j-1}, U_{j-1} \rangle \langle Y_1, W \rangle \langle Y_2, \emptyset \rangle \cdots \langle Y_q, \emptyset \rangle \langle X_{j+1}, U_{j+1} \rangle \cdots \langle X_h, U_h \rangle.$$

By (1) in the algorithm, W is of the form $W = U_j \cup \text{alph}(y_0 y_1 \cdots y_q)$, where $y_i \in V^*$, for all i, $1 \leq i \leq q$, and $X_j \to y_0 Y_1 y_1 \cdots Y_q y_q \in P$. Therefore,

$$x_0 X_1 x_1 \cdots X_j x_j \cdots X_h x_h \Rightarrow_G$$
$$x_0 X_1 x_1 \cdots X_{j-1} x_{j-1} y_0 Y_1 y_1 \cdots Y_q y_q x_j X_{j+1} x_{j+1} \cdots X_h x_h.$$

Clearly,

$$\left(\bigcup_{1 \leq i \leq h} U_i\right) \cup \left(\bigcup_{0 \leq i \leq q} \text{alph}(y_i)\right) \subseteq$$
$$\left(\bigcup_{0 \leq i \leq h} \text{alph}(x_i)\right) \cup \left(\bigcup_{0 \leq i \leq q} \text{alph}(y_i)\right).$$

(ii) Let $\langle X_j, U_j\rangle \to \langle X_j, W\rangle \in P'$ be a rule introduced in (2) in the algorithm, for some j, $1 \le j \le h$, where $W \subseteq V$, so

$$\langle X_1, U_1\rangle\langle X_2, U_2\rangle \cdots \langle X_j, U_j\rangle \cdots \langle X_h, U_h\rangle \Rightarrow_H \langle X_1, U_1\rangle\langle X_2, U_2\rangle \cdots \langle X_j, W\rangle \cdots \langle X_h, U_h\rangle.$$

By (2) in the algorithm, W is of the form $W = \big(U_j - \{Y\}\big) \cup \mathrm{alph}(y)$, where $Y \in V$, $y \in V^*$, and $Y \to y \in P$. Recall that $\bigcup_{1\le i\le h} U_i \subseteq \bigcup_{0\le i\le h} \mathrm{alph}(x_i)$ by the induction hypothesis. Since $Y \in \bigcup_{1\le i\le h} U_i$, some x_k has to be of the form $x_k = x'_k Y x''_k$, where $x'_k, x''_k \in V^*$, so

$$x_0 X_1 x_1 \cdots X_k x_k \cdots X_h x_h \Rightarrow_G x_0 X_1 x_1 \cdots X_k x'_k y x''_k \cdots X_h x_h.$$

Clearly,

$$\big(\bigcup_{1\le i\le h, i\ne j} U_i\big) \cup \big(U_j - \{Y\}\big) \cup \mathrm{alph}(y) \subseteq \big(\bigcup_{1\le i\le h, i\ne k} \mathrm{alph}(x_i)\big) \cup \big(\mathrm{alph}(x_k) - \{Y\}\big) \cup \mathrm{alph}(y).$$

Observe that these two cases cover all possible derivations of the form $x \Rightarrow_H w$. Therefore, the claim holds. □

Next, we establish the identity $L(H) = L(G)$. Consider a special case of Claim 1 when $x_i = \varepsilon$, $X_j \in T$, for all i and j, $0 \le i \le h$, $1 \le j \le h$, for some $h \ge 1$. Then, $S \Rightarrow_G^* X_1 X_2 \cdots X_h$ implies that $\langle S, \emptyset\rangle \Rightarrow_H^* \langle X_1, \emptyset\rangle\langle X_2, \emptyset\rangle \cdots \langle X_h, \emptyset\rangle$. By the initialization part of the algorithm, $\langle X_j, \emptyset\rangle \to X_j \in P'$, for all j, $1 \le j \le h$, so

$$\begin{aligned} \langle S, \emptyset\rangle &\Rightarrow_H X_1\langle X_2, \emptyset\rangle \cdots \langle X_h, \emptyset\rangle \\ &\Rightarrow_H X_1 X_2 \cdots \langle X_h, \emptyset\rangle \\ &\ \ \vdots \\ &\Rightarrow_H X_1 X_2 \cdots X_h. \end{aligned}$$

Hence, $L(G) \subseteq L(H)$. Let $z \in L(H)$. By Claim 2, $\langle S, \emptyset\rangle \Rightarrow_H^* x \Rightarrow_H^* z$, where $x \in V'^+$. By Claim 3, $S \Rightarrow_G^* z$. Therefore, $L(H) \subseteq L(G)$, and the theorem holds. □

4 Concluding Remarks

In this final section, we discuss the applicability of our algorithm to other derivation modes in E0S grammars. Then, we propose two open problems to consider in the future investigation related to the subject of this paper.

4.1 Semi-Parallel and Parallel Derivation Modes

During every derivation step in an E0S grammar, a single symbol is rewritten. Hence, these grammars work under a *sequential derivation mode*. We next define a generalization of this mode, where some symbols are simultaneously rewritten while others remain unrewritten (like in scattered context grammars, see [1]).

Let $G = (V, T, P, S)$ be an E0S grammar. G makes a *semi-parallel derivation step* from $u_0v_1u_1 \cdots v_nu_n$ to $u_0w_1u_1 \cdots w_nu_n$, denoted by

$$u_0v_1u_1 \cdots v_nu_n \text{ s-par}\Rightarrow_G u_0w_1u_1 \cdots w_nu_n$$

if and only if $u_i \in V^*$ for all $i = 1, \ldots, n$, $v_j, w_j \in V^*$, and $v_j \Rightarrow_G w_j$ for all $j = 1, \ldots, n$, for some $n \geq 1$. Let $\text{s-par}\Rightarrow_G^*$ denote the reflexive-transitive closure of $\text{s-par}\Rightarrow_G$. The *language generated by G under the semi-parallel mode* is denoted by $L(G, \text{s-par}\Rightarrow_G)$ and defined as

$$L\big(G, \text{s-par}\Rightarrow_G\big) = \big\{w \in T^* \mid S \,\text{s-par}\Rightarrow_G^* w\big\}.$$

The following theorem says that Algorithm 1 is applicable to E0S grammars working under this mode. Let us note that the standard algorithm also works for this mode.

Theorem 2. Let G be an E0S grammar. Algorithm 1 halts and correctly converts G to a propagating E0S grammar H satisfying $L(G, \text{s-par}\Rightarrow_G) = L(H, \text{s-par}\Rightarrow_H)$.

Proof. This theorem can be established by analogy with the proof of Theorem 1, so we leave its proof to the reader. □

By analogy with the definition of the semi-parallel mode, we may define a *parallel mode*, where during a single derivation step, all occurrences

of symbols in the current sentential form have to be rewritten. However, observe that neither Algorithm 1 nor the standard algorithm are applicable to E0S grammars working under this mode. To remove erasing rules from E0S grammars working under the parallel mode, we may use the algorithm for the elimination of erasing rules in E0L systems (see pages 63–65 in [10]).

4.2 Open problems

We close this paper by proposing two open problems.

I. Observe that there exist other derivation modes under which the algorithm achieved in the previous section does not work properly. For instance, the algorithm is inapplicable to the Indian derivation mode (see [7], [8], or Section 2.4 in [12]). Recall that an Indian derivation step is performed so a rule is selected, and all symbols coinciding with the left-hand side of this rule are rewritten by it in the current sentential form. Consider the Indian parallel grammar having the three rules $S \to SS$, $S \to a$, and $S \to \varepsilon$, where S is a nonterminal and a is a terminal. Obviously, its language equals

$$\left\{ a^{2^n} \mid n \geq 0 \right\} \cup \{\varepsilon\}.$$

If we convert this grammar to another Indian parallel grammar by Algorithm 1, the resulting Indian grammar generates $\{a^n \mid n \geq 1\}$, which differs from $\{a^{2^n} \mid n \geq 0\}$. As a result, the algorithm is inapplicable to derivation modes that involve the Indian derivation mode, such as the mode of Russian parallel grammars (see [4] or Section 2.4 in [12]). Also, note that our algorithm is not applicable to the mode of k-grammars, where at every derivation step, exactly k occurrences of symbols have to be simultaneously rewritten (see [5], [6] and page 126 in the second volume of [11]). Can we modify Algorithm 1 so it works under these derivation modes as well? Recall that it is an open problem whether we can always eliminate all erasing rules from any Russian parallel grammar or from any k-grammar.

II. Compared to its input grammar, the output grammar produced by Algorithm 1 has many more symbols and rules. To be precise, the cardinality of symbols and rules of output grammar has an exponential

increase from the cardinality of symbols and rules of input grammar. Can we improve this algorithm so it works in a more economical way?

5 Funding

This work was supported by The Ministry of Education, Youth and Sports of the Czech Republic from the National Programme of Sustainability (NPU II), from the project IT4Innovations excellence in science—LQ1602.

6 Acknowledgement

We are grateful for comments made by Petr Zemek and the anonymous referee of this paper.

References

[1] S. A. Greibach and J. E. Hopcroft, "Scattered context grammars," *Journal of Computer and System Sciences*, vol. 3, no. 3, pp. 233–224, August, 1969.

[2] H. C. M. Kleijn, "Basic ideas of selective substitution grammars," *Lecture Notes in Computer Science*, vol. 281, pp. 75–95, 1987.

[3] H. C. M. Kleijn and G. Rozenberg, "Context-free like restrictions on selective rewriting," *Theoretical Computer Science*, vol. 16, no. 3, pp. 237–269, 1981.

[4] M. K. Levitina, "On some grammars with global productions," *NTI*, vol. 2, no. 3, pp. 32–36, 1972. (in Russian)

[5] K. Salomaa, "Hierarchy of k-context-free languages, part 1," *International Journal of Computer Mathematics*, vol. 26, no. 2, pp. 69–90, Mar, 1989.

[6] K. Salomaa, "Hierarchy of k-context-free languages, part 2," *International Journal of Computer Mathematics*, vol. 26, no. 3, pp. 193–205, Mar, 1989.

[7] R. Siromoney and K. Krithivasan, "Parallel context-free languages," *Information and Control*, vol. 24, no. 2, pp. 155–162, 1974.

[8] S. Skyum, "Parallel context-free languages," *Information and Control*, vol. 26, no. 3, pp. 280–285, 1974.

[9] A. Meduna, *Automata and Languages: Theory and Applications*, London, Springer, 2000.

[10] G. Rozenberg and A. Salomaa, *Mathematical Theory of L Systems*, Orlando, Academic Press, 1980.

[11] *Handbook of Formal Languages, Volumes I through III*, G. Rozenberg, A. Salomaa, Eds. New York, Springer, 1997.

[12] J. Dassow and G. Paun, *Regulated Rewriting in Formal Language Theory*, New York, Springer, 1989.

Alexander Meduna, Martin Havel

Received February 2, 2022
Accepted March 17, 2022

Alexander Meduna
Faculty of Information Technology, Brno University of Technology
Božetěchova 1/2, 612 66 Brno, Czech Republic
E–mail: meduna@fit.vutbr.cz

Martin Havel
Faculty of Information Technology, Brno University of Technology
Božetěchova 1/2, 612 66 Brno, Czech Republic
E–mail: xhavel44@stud.fit.vutbr.cz

Vehicle Detection from Unmanned Aerial Images with Deep Mask R-CNN

Rıdvan Yayla, Emir Albayrak, Uğur Yüzgeç

Abstract

In this paper, a classification approach which is applied to Mask Region-based Convolutional Neural Network as deeper is proposed for vehicle detection on the images from UAV instead of the familiar methods. The different types of unmanned aerial vehicles are widely used for a lot of areas such as agricultural spraying, advertisement shooting, fire extinguishing, transportation and surveillance, exploration, destruction for the military. In recent years, deep learning techniques are progressively developed for object detection. Segmentation algorithms based on CNN architecture are especially widely used for extracting meaningful parts of an image. Additionally, Mask R-CNN based on CNN architecture rapidly detects the object with high-accuracy on an image. This study shows that the high-accuracy results are obtained when the Mask R-CNN is applied as deeper in vehicle detection on the images taken by UAV.

Keywords: Convolutional neural networks, Deep learning, Mask R-CNN, Vehicle detection.

1 Introduction

Nowadays, the images and the videos that are received from unmanned aerial vehicles (UAV) are widely used in a lot of areas such as commerce, agriculture, security, and the military. The vehicles or moving objects are mostly taken notice of for object detection due to the security and their variations. The vehicle detection is especially required when a moving target is detected for learning its coordinates in a military operation. Moreover, the incoming vehicles are directed to the free

©2022 by CSJM; R.Yayla, E.Albayrak, U.Yüzgeç
doi:10.56415/csjm.v30.09

parking areas when a vehicle intensity rate is determined in an open-top car parking. Additionally, illegal structures can also be detected with deep learning algorithms by comparing them to the previous drone images.

Deep learning, which is a branch of machine learning, is basically an increased layer in the number of hidden layers of Multi-Layer Perceptron (MLP) by a large number [1]. In recent years, region-based segmentation model based on Convolutional Neural Network (CNN) architecture is an effective solution for object detection. Region-based Convolutional Neural Network (R-CNN), Fast R-CNN, Faster R-CNN and Mask R-CNN are the most used models for object detection. In this study, the accuracy of vehicle detection from a UAV image is evaluated by comparing Mask R-CNN models based on different backbone networks with pre-trained weights such as Resnet-101, Vgg16, (Microsoft) MS Coco. When a deeper Mask R-CNN algorithm is used for vehicle detection, the better results are obtained for the vehicle segmentation.

2 Methodology

Object recognition is a scientific field, which is related to computer vision and image processing, that deals in visual images and videos with the detection of instances of semantic objects of an exact type (such as traffic light, cars, or person). There are a lot of object detection applications that include image and video improvement in many fields of computer vision. Deep learning methods have been commonly used in the last decade for object detection. The most well-known and used techniques are R-CNN, Fast R-CNN, Faster R-CNN and Mask R-CNN for object detection. Additionally, YOLO algorithm based on CNN architecture that is also used for non-dynamic images is especially used for real-time video images. Li et al. developed a YOLO-Grape model for real-time detection of multiple varieties of table grapes in complex situations [2]. Lin and Li developed an integrated circuit board object Model based on YOLO for fast quality management process [3]. These studies are based on real-time object detection but the YOLO algorithm just uses a bounding box for object detection and the performance of the YOLO is compared by Fast R-CNN that is the previous

version of Mask R-CNN. The advantage of Mask R-CNN is to segment objects as a whole with masking.

Nie et al. realized an inshore ship detection based on Mask R-CNN by integrating to Soft-Non-Maximum Yang. They improved to ship segmentation with their proposed method by using instance segmentation on Mask R-CNN [4]. Li and Cheng developed a pedestrian detection application based on Mask R-CNN. In their study, they determined weak points of Mask R-CNN and they optimized their own network based on Mask R-CNN. By this way, they have provided a quality pedestrian gender segmentation with their own created dataset [5]. Moreover, Vemula and Frye proposed a study that is related to power-line detection by using UAV images. They improved Mask R-CNN detection by transfer learning and Mask R-CNN powerline detector is proposed based on UAV images [6]. Song and Zhao have used "Mask R-CNN" for the gastric cancer diagnosis from the medical images. Instead of the well-known object detection, they optimized different size medical images for the pathological experiments and obtained successful results on gastric cancer detection [7].

As it is seen in the actual examples, the Mask R-CNN can be effectively optimized with different methods and it is used for the different purposes from security to health. In our study, the vehicles on UAV images are segmented by using Mask R-CNN as deeper.

2.1 Convolutional Neural Network (CNN)

CNN is a powerful deep learning model for object detection and it provides high accuracy in recent years. CNNs consist of neurons with renewable weights and biases [8]. Each neuron takes some inputs and realizes a dot product and arbitrarily follows it with a non-linearity after these steps. There are six common layers in the CNN architecture, and these layers are as given below [9]:

- Image Input Layer
- Convolutional Layer
- Rectified Linear Unit (ReLu)
- Pooling Layer
- Fully Connected Layer

• Classification (Softmax) Layer

The image which consists of the pixels is converted to matrix format in the image input layer. In the convolutional layer, a field of the image is handled and a convolution operation is performed with a small part of the input matrix having the same dimension. An activation function is used to get rid of the negative values generated during the convolution process. Because the non-negative values are not generated, the Rectified Linear Unit (ReLU) is the basically used activation function in deep learning architecture. The ReLu function is given in the equation (1) [9].

$$\mathrm{ReLu}(x) = \begin{cases} 0 \text{ if } x < 0 \\ x \text{ if } x \geq 0 \end{cases}. \tag{1}$$

In the CNN architecture, the pooling layers are periodically added to the network. The pooling layer is independently executed in each depth slice of the input and it is resized by using max operation. According to this process, pooling layer is also called max pooling layer. The aim of the max operation is to decrease the number of parameters and calculations in the network.

In the fully connected (dense) layer, all neurons are fully connected to each other with all activations in the previous layer. The aim of the fully connected layers is basically feature extraction and classification. The predictions in dense layer are ready for the classification layer. The classification layer is a standard fully-connected (dense) layer that uses the softmax activation function. In this final layer, a prediction of classes that are created in the training model is made for the desired field of an image via the softmax function. The softmax function is given in the equation (2) [9].

$$s\left(x_i\right) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}}. \tag{2}$$

Most of the application which is made by using Mask R-CNN is focused on medical, radar image, or object detection. In our study, the vehicle images that are taken from a UAV are segmented by using a deeper Mask R-CNN algorithm.

2.2 Region-based Segmentation

2.2.1 R-CNN

Girschick et al. developed an object detection method that can be implemented from high-capacity CNNs to region proposals so as to situate and segment objects in 2014 [10]. They proposed a method with using the selective search algorithm that takes out only 2000 regions from the image. These regions are called region proposals. The CNN is set to region proposals of the image, and a prediction is generated by the CNN. This method is called region-based convolutional neural network (R-CNN). The working principle of the R-CNN is summarized as follows:

- A region proposal in an image is sent to CNN architecture and the correct region is found.
- The region proposal is classified by using an operation that is called a selective search algorithm. The algorithm provides the analysis of the image by different-size windows that try to combine neighbor pixels by texture or color intensity.
- Selective search is executed on the image for finding the desired region.
- The obtained regions from the selective search algorithm are utilized for classification and feature extraction by using a pretrained CNN architecture.

R-CNN obtains perfect object detection correctness by using CNN for image classification but has mostly disadvantages. Because all the proposed regions are applied to CNN, the running time of the algorithm is long and more memory is required. The Fast R-CNN model based on R-CNN is developed for removing these disadvantages.

2.2.2 Fast R-CNN

R-CNN works very well for detecting an object but it is slow because of the fact that the Selective Search algorithm is used for determining

region proposals. In the R-CNN model, all the region proposals are delivered to ConvNet architecture, and it runs for all region proposals. Instead of that 2000 regions are to feed to CNN architecture, the convolution operation is made only once per image in Fast R-CNN and a feature map is extracted from it. In the convolutional feature map, the desired regions are recognised and are scanned into squares by using a kind of pooling layer that performs max pooling on inputs [11]. By this way, the desired regions are resized into a fixed size for setting into a fully connected layer. Each region proposal pursues on ConvNet architecture, and this method is called Region of Interest (ROI) Pooling; this kind of pooling layer is called Region of Interest (RoI) layer. By the RoI pooling, the region is divided into subregions. The RoI Pooling extracts a fixed-size frame from the feature map and uses the attributes for gaining the final class label and bounding box. [12]. The output attributes from the RoI Pooling layer are delivered into the sequential Fully Connected layers, the softmax and bounding box (BB) regression branches. Each RoI expresses the number of categories and a single background category. The softmax classification produces probability values of each RoI. The BB regression output is used for making bounding boxes from the region proposal algorithm more susceptible.

2.2.3 Faster R-CNN

Faster-CNN was developed for eliminating computing and running time in 2016. Shaoqing et al. developed an object detection algorithm that provides the network learning of region proposals [13]. The selective search algorithm is not used in the new approach due to the object detection algorithm. In this model, a discrete network is used to predict the region proposals in place of using the selective search algorithm on the feature map to recognize the region proposals. The network is called as Region Proposal Network (RPN).

Faster R-CNN consists of two modules. The first module proposes the regions by using deep fully ConvNets, and the second one uses region proposals via the Fast R-CNN detector [14]. The Faster R-CNN architecture is shown in Figure 1. Faster R-CNN uses the same convolutional network for both region proposal production and object detec-

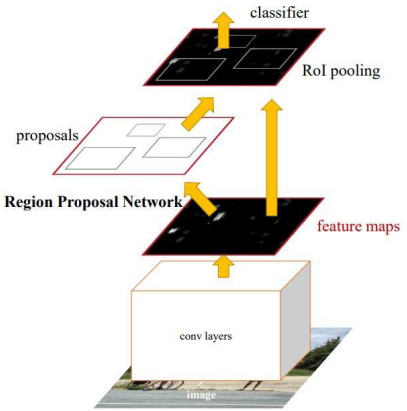


Figure 1. Architecture of the Faster R-CNN [13]

tion. Unlike the selective search algorithm, it is divided into ConvNets and the Region Proposal Network (RPN) which depends on the determined attributes of the image [15]. This method provides a decrease in the computing process and higher accuracy results.

2.2.4 Mask R-CNN

Mask Region-based Convolutional Neural Network (Mask R-CNN) is a segmentation model based on Faster R-CNN model. Mask R-CNN provides that the network not only performs object detection but pixel-wise instance segmentation based on semantic segmentation. While the model predicts a bounding box recognition by this method, it adds a mask to object at the same time. Mask R-CNN is performed on some principles. These principles are listed as follows [16]:

- It works on Faster R-CNN model by inserting a parallel branch.
- It predicts segmentation mask by using a small (Fully Connected Layer) FCN.
- It performs better than state-of-art models in person keypoint detection, segmentation and bounding box detection.
- It changes RoIs in Faster R-CNN to a quantization-free layer

called RoI Align. RoI Align removes the quantization which causes the misalignment. 4 locations are sampled and bilinear interpolation is used.

• The separated networks run in parallel, and in this way, the prediction system runs at a higher speed.

• It uses an instance segmentation method that is based on semantic segmentation. The difference between these segmentation methods is as follows: while the semantic segmentation segments (classifies) the same objects into a single one with one label (person, car, etc.), the instance segmentation segments (classifies) the same objects as similar instances with different labels such as person1, person2, or car1, car2.

The Mask R-CNN is different from prior systems, where classification depends on mask prediction. It also uses the lost function for fixing weight errors. The lost function (L) for each sampled RoI is calculated as follows [16].

$$L = L_{cls} + L_{box} + L_{mask}. \tag{3}$$

In equation (3), L_{cls} expresses the classification loss, L_{box} is the bounding box loss, and L_{mask} is the masking loss. RoIPool is a useful process for exposing a small feature map such as 7×7 from each RoI [17]. RoI Align abolishes the harsh quantization of RoI Pool by aligning the determined features with the input. The bilinear interpolation which computes the exact values of the input features at four regularly sampled locations in each RoI bin and aggregates the result (using max or average) is used in this model [16][17]. The Mask R-CNN differs from the Faster R-CNN with two features.

• Masking: Faster R-CNN consists of two common features which are bounding box and prediction of object detection. The masking feature is added in the Mask R-CNN algorithm.

• Instance segmentation: If there are two same objects or same meaningful parts in an image, these objects or parts are divided into different masking or colourization [17]. Mask R-CNN uses a fully connected network to predict the mask.

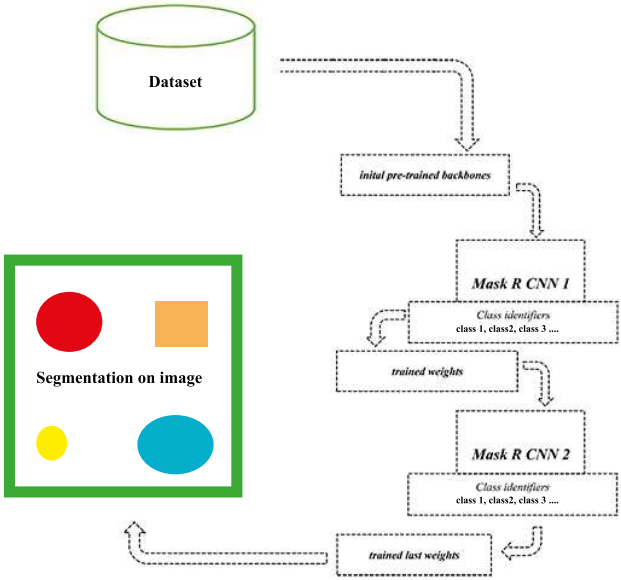


Figure 2. Working principle of Deep Mask R-CNN [18]

2.3 Deep Mask R-CNN

In [18], a multi-class hybrid classification method is proposed by using deep Mask R-CNN for smoothed Synthetic Aperture Radar (SAR) images. The method is trained with different backbone networks that are integrated with Deep Mask R-CNN, and these networks are compared to each other. When the Mask R-CNN is trained with default (pre-trained) backbone weights such as MS coco, inception v3, vgg16 resnet101 and resnet50, a new trained weights are obtained by Mask R-CNN at the end of the training process. The working principle of deep Mask R-CNN is shown in Figure 2. The segmentation of the meaningful parts is observed in the image after the pre-trained backbone weights are given first convolutional inputs in the initial running time. If the segmentation loss values are not sufficiently low, the obtained trained weights are repeatedly sent to Mask R-CNN within a new training process. The deep convolutional process is repeated until

the segmentation losses reach a constant low value.

The deep Mask R-CNN aims to decrease Mask R-CNN algorithm losses and to obtain a quality segmentation that is properly separated from each other [19]. According to the related work, it is shown that when the Mask R-CNN applied deeper to an image, the Mask R-CNN losses are decreased and more high-quality segmentation is obtained. In our study, the Deep Mask R-CNN, which is the second hybrid study of the related work, is used for a quality vehicle segmentation by decreasing Mask R-CNN algorithm losses.

3 System Design and Components

3.1 Materials

In this study, vehicle detection from the UAV is realized by applying to Mask R-CNN as deeper. The vehicles in the image can be detected with instance segmentation at the end of the training process.

The DJI Mavic PRO model drone, which has a 12.3 MP resolution camera supported CMOS sensor, is used as the UAV [20]. The drone can also take 1080p, 4K and HD camera shooting. The drone used in this study is shown in Figure 3. In this study, 282 images taken from

Figure 3. UAV used in this study (DJI Mavic PRO) [20]

the UAV trained with the Mask R-CNN algorithm (1000 iterations at each step and 50 iterations in total) and the vehicles in the UAV image

were detected as a bird's-eye. The images are pictures that mostly contain vehicles and are taken from different angles and locations. The images are initially divided into two parts as test and train datasets. The vehicles in all images are polygonally drawn with the VGG image annotator, which is a basic and useful drawing tool [21].

Additionally, the study is realized with hardware which is Nvidia Geforce GTX 1070 Ti (8GB – GDDR5), 16 GB RAM, GPU, Intel (R) Core (TM) 4 cores CPU and 240 GB SSD + 1 TB Harddisk [22]. The experiment is also realized by Tensorflow and Keras libraries based on Python language. Moreover, Tensorboard graphic interface at Tensorflow library is used for determining error rates at the end of the training. By this way, the observation of the error rates due to the iterations can be made at Ubuntu platform. At the same time, the different images, which were taken from different locations as the eye-bird view on the web and not taken from the UAV, were also tested in the test process.

3.2 Methods

Nowadays, deep learning tools based on advanced graphic cards have become very popular for the object-detection in computer vision. The deep learning libraries such as Tensorflow, Keras are very useful platforms for applying to deep learning model [23]. The image is taken by the deep learning platforms and it is converted to numpy arrays which are defined in Tensorflow library.

The Mask R-CNN algorithm loss should be decreased in Mask R-CNN for a high-quality segmentation. When the Mask R-CNN algorithm is applied for the vehicle segmentation with the default backbones such as MS Coco, Resnet-50, vgg16, a segmentation weight file is obtained at the end of the last iteration of 1^{st} training process [24]. The segmentation losses are observed with the obtained weights and the 2^{nd} training process is started with these weights for decreasing the losses. The Deep Mask R-CNN is a useful method for decreasing the algorithm loss by using the trained weights. The segmentation is observed at the end of each training process until the segmentation edges can be improved. The working principle of the proposed method is shown in Figure 4. The proposed method can also be repeated more

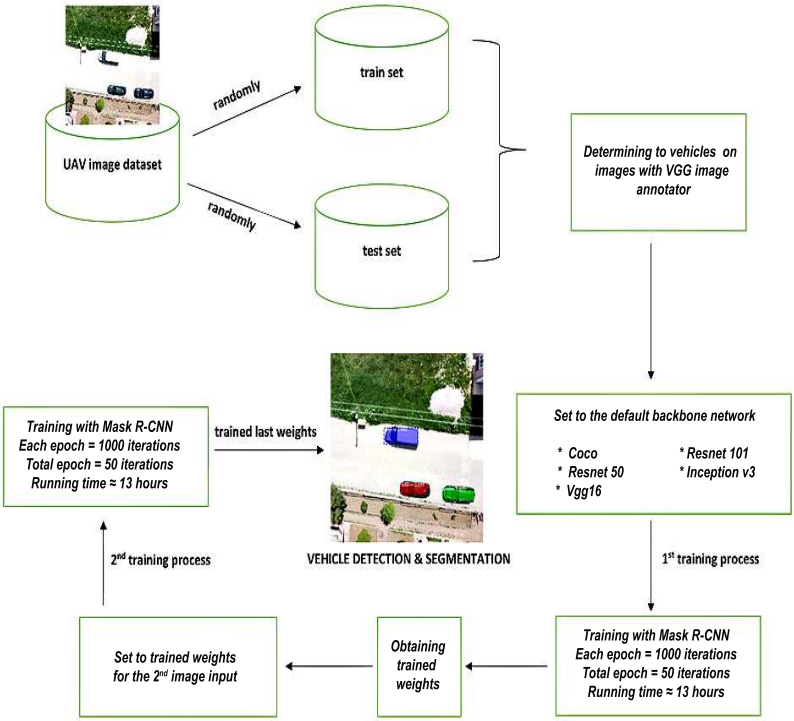


Figure 4. Working principle of the proposed method

than two times until the accuracy of the edges reaches the least error. When the Mask R-CNN loss reaches a constant value at the end of the training process, the experiment is ended.

The loss values are variants for different segmentation experiments. In our study, the single-vehicle class is defined for the segmentation and the Mask R-CNN scans vehicle fields of the image in the algorithm. Thanks to instance segmentation, more than one vehicle can be detected with different colorization in the deep Mask R-CNN. In this way, vehicles are distinguished from each other in the image.

The method is not only applied to static images but it can also be applied to dynamic images such as video and gif extension images. YOLO algorithm based on CNN is faster for the dynamic images but it uses only bounding boxes for the vehicles segmentation [25]. In our study, because the masking and instance segmentation are used in Mask R-CNN, the Mask R-CNN is preferred for a high-quality vehicle segmentation. The vehicles can be segmented with different masking in the deep Mask R-CNN.

3.3 Experimental Results and Performance

When the proposed method is applied to different pre-trained backbone networks, the performances are observed for each backbone weight. Each experiment is trained with different backbones and the trained weights, which are obtained at the end of the 1st training, are sent to the network as the initial weights again. The aim of the deep Mask R-CNN is to decrease Mask R-CNN losses which consist of the masking loss, classification loss, and bounding box loss for a high-quality segmentation.

The classification models that are used in the study have different performances. Ms Coco model is the default (baseline) standard pre-trained model for object detection. The more higher accuracy has been obtained in the preliminary Ms Coco model due to the large-scale dataset for the various computer vision detection. The experiment has been initially executed for the default Ms Coco model. After the default model, the experiment is executed for the other pre-trained models for the performance comparison. For example, while the Vgg16 backbone

network model has fixed-size kernels for the experiment of the study, the Inception v3 model has wider – parallel kernels for the experiment of the study. Skipping connection between the perceptions is a technic that is used in the Resnet models. Resnet models have different parameter numbers and the Resnet-50 has fewer parameters. Due to the skipping technique and fewer parameters, the Resnet-50 network model has provided the most successful results for the experiment.

The four sample images that are taken from two different UAVs and locations are shown in Figure 5. The segmentation results are also shown in Figure 6, Figure 7, Figure 8, Figure 9 and Figure 10. In the experiment figures, the bounding boxes, masking, and prediction accuracy are shown for each vehicle. The accuracy values of each vehicle detection are also shown in top-right of the each detected vehicle as numerical according to related backbone accuracy of the experiments.

Figure 5. Sample Images (Location: Pazaryeri-Bilecik and Turgutlu-Manisa Turkey [26])

The Deep Mask R-CNN experimental results are shown in Table 1. In Table 1, five different backbone network performances are shown

Figure 6. Deep Mask R-CNN (Ms Coco) segmentation (accuracy 92%)

with accuracy and loss. Each pre-trained model is initially sent to CNN at the 1st iteration and the observed weights are also sent to CNN at the 2nd iteration. This recurrent process is applied until the loss function arrives at a fixed value. In this study, the loss values have arrived at a fixed value in the 2nd iteration. In Table 1, the fixed values of a total loss, classification, bounding box, and masking loss are shown in the 2nd iteration. The obtained accuracy is also shown in the 2nd iteration for each backbone network.

3.4 Conclusion

Deep learning techniques are widely used nowadays for a lot of areas such as image processing, natural language processing, network security. In our study, the vehicle detection is made with a deeper Mask R-CNN based on CNN deep learning architecture by using the images, which are obtained from a UAV. A single-class segmentation based on the vehicle is made by using instance segmentation feature of the Mask R-CNN. Thanks to this feature, multi vehicles of an image are seg-

Figure 7. Deep Mask R-CNN (Resnet-50) segmentation (Accuracy: 93%)

Figure 8. Deep Mask R-CNN (Vgg16) segmentation (Accuracy: 88%)

Figure 9. Deep Mask R-CNN (Resnet-101) segmentation (Accuracy: 71%)

Figure 10. Deep Mask R-CNN (Inception-v3) segmentation (Accuracy: 88%)

Table 1. The experimental results for pre-trained backbones.

Mask R-CNN (1st iteration)					
Backbone	***loss***	***mrcnn class loss***	***mrcnn bbox loss***	***mrcnn mask loss***	***Accuracy***
Vgg16	0.1948	0.02296	0.02176	0.101	80%
Inception v3	0.1875	0.02375	0.02061	0.0987	81%
Resnet 101	0.4635	0.05099	0.06606	0.1771	53%
Resnet 50	0.08741	0.01473	5.0135	0.05257	91%
Ms Coco	0.08652	0.01478	4.9783	0.05138	91%
Mask R-CNN (2nd iteration)					
Backbone	***loss***	***mrcnn class loss***	***mrcnn bbox loss***	***mrcnn mask loss***	***Accuracy***
Vgg16	0.1118	0.01413	0.01053	0.0668	88%
Inception v3	0.1151	0.01525	0.01026	0.06763	88%
Resnet 101	0.2899	0.03569	0.03697	0.1225	71%
Resnet 50	0.06656	0.01172	3.8966	0.04082	93%
MS Coco	0.08036	0.01371	4.9783	0.04938	92%

mented with different segmentation and all vehicles in the image are separated from each other. It is aimed that the segmentation loss is decreased by using Mask R-CNN as deeper. In this study, a prototype experiment is made for vehicle detection. If more images are trained and the dataset image diversity becomes more than the current diversity, the accuracy of the detection is greater. Moreover, the dataset images have been taken on sunny days and the models are trained by these sunny images. Vehicle detection can be affected by other weather conditions. The study can be expanded for other weather conditions by being trained in different images such as cloudy, rainy, or foggy weather images. This study also provides ease of use for vehicle detection in many areas. It can also be extended with multi-class segmentation such as buildings, vehicles, and roads. Thanks to multi-class segmentation, different moving objects can be detected with the proposed method.

4 Acknowledgement

The study called "Vehicle Detection from Unmanned Aerial Vehicle Images with Deep Mask R-CNN" has been made in the scope of Bilecik Şeyh Edebali University, Graduate Education Institute, master thesis study.

References

[1] J. Brownlee, "What is Deep Learning," Machine Learning Mastery, Aug. 14, 2019. [Online]. Available: https://machinelearningmastery.com/what-is-deep-learning/

[2] H.Li, C. Li, G. Li, and L. Chen, "A real-time table grape detection method based on improved YOLOv4-tiny network in complex background," *Biosystems Engineering*, vol. 212, pp. 347–359, 2021.

[3] L. Szu-Yin and L. Hao-Yu "Integrated Circuit Board Object Detection and Image Augmentation Fusion Model Based on YOLO," *Frontiers in Neurorobotics* , vol. 15, pp. 155, 2021.

[4] S. Nie, Z. Jiang, H. Zhang, B. Cai, and Y. Yao, "Inshore Ship Detection Based on Mask R-CNN," in *Proc. 2018 IEEE International Geoscience and Remote Sensing Symposium*, (Valencia), 2018, pp. 693–696.

[5] X. Li and S. Cheng, "Pedestrian Gender Detection Based on Mask R-CNN," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, (Chengdu), 2019, pp. 2082–2086.

[6] S. Vemula and M. Frye, "Mask R-CNN Powerline Detector: A Deep Learning approach with applications to a UAV," in *Proc. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, (San Antonio), 2020, pp. 1–6.

[7] G. Cao, W. Song, and Z. Zhao, "Gastric Cancer Diagnosis with Mask R-CNN," in *Proc. 2019 11th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, (Hangzhou), 2019, pp. 60–63.

[8] A. Deshpande, "A Beginner's Guide To Understanding Convolutional Neural Networks," UCLA CS'19, Jul. 29, 2016. [Online]. Available: https://adeshpande3.github.io/adeshpande3.github.io/

[9] R. Yayla and B. Şen, "Research on Region-Based Convolutional Neural Network for Semantic Segmentation," in *Proc. 8th International Conference on Advanced Technologies Conference (ICAT'19)*, (Sarajevo), 2019, pp. 244–249.

[10] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation," in *Proc. 2014 IEEE Conference on Computer Vision and Pattern Recognition*, (Columbus, OH, USA), 2014, pp. 580–587.

[11] S. Hsu, C. Huang, and C. Chuang, "Vehicle detection using simplified fast R-CNN," in *Proc. 2018 International Workshop on Advanced Image Technology (IWAIT)*, (Chiang Mai), 2018, pp. 1–3.

[12] R. Girshick, "Fast R-CNN," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition(ICCV)*, (Santiago), 2015, pp. 1440–1448.

[13] R. Shaoqing, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," *Proc. IEEE,* vol. 39, no. 6, pp. 1137–1149, Jun 2017.

[14] B. Liu, W. Zhao and Q. Sun, "Study of object detection based on Faster R-CNN," in *Proc. 2017 Chinese Automation Congress (CAC)*, (Jinan), 2017, pp. 6233–6236.

[15] J. Lin, C. -. T. Chiu, and Y. Cheng, "Object Detection with Color and Depth Images with Multi-Reduced Region Proposal Network and Multi-Pooling," in *Proc. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, (Barcelona), 2020, pp. 1618–1622.

[16] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," in *Proc. 2017 IEEE International Conference on Computer Vision (ICCV)*, (Venice), 2017, pp. 2980–2988.

[17] R.Yayla and B. Şen, "Region-based Segmentation of Terrain Fields in SAR Images," in *Proc. 28th Signal Processing and Communications Applications Conference Conference (SIU2020)*, Gaziantep, 2019, pp. 1–4.

[18] R. Yayla and B. Şen "A New Classification Approach with Deep Mask R-CNN for Synthetic Aperture Radar Image Segmentation," *Elektronika Ir Elektrotechnika*, vol. 26, no. 6, pp. 52–57, 2020.

[19] C. Ozcan, B. Sen, and F. Nar, "Sparsity-Driven Despeckling for SAR Images," *IEEE Geoscience and Remote Sensing Letters*, vol. 13, no. 1, pp. 115–119, 2016.

[20] *DJI Mavic Pro User Manual*, DJI technology., Shenzhen, China, 2017.

[21] A. Dutta and A. Zisserman, "The VIA annotation software for images,audio and video," in *Proc. 27th ACM International Conference on Multimedia*, (Nice), 2019, pp. 2276-–2279.

[22] R. Yayla, "Hybrid Intelligent Classification Technique For High-Resolution Sar (Synthetic Aperture Radar) Images," Ph.D. dissertation, Dept. Comp. Eng., Ankara Yıldırım Beyazıt Univ., Ankara, Turkey, 2020.

[23] Z. Zeng, Q. Gong, and J. Zhang, "CNN Model Design of Gesture Recognition Based on Tensorflow Framework," in *Proc. IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, (Chengdu), 2019, pp. 1062–1067.

[24] W. Abdulla, "Mask R CNN for object detection and instance segmentation on Keras and TensorFlow,"

GitHub repository, Mar. 20, 2017. [Online]. Available: https://www.github.com/matterport/Mask_RCNN

[25] M. Liu, X. Wang, A. Zhou, et al., "UAV-YOLO: Small Object Detection on Unmanned Aerial Vehicle Perspective," *Sensors Journal*, vol. 20, no.81, pp. 1–12, 2020.

[26] M. Almislar, "Manisa Turgutlu (Town) 4k aerial view," Youtube, Sep. 5, 2019. [Online]. Available: https://www.youtube.com/watch?v=AFwPmWeUwpM (in Turkish)

Rıdvan Yayla, Emir Albayrak,
Uğur Yüzgeç

Received February 22, 2021
Revised version December 29, 2021
Accepted for publication February 1, 2022

Rıdvan YAYLA
Computer Engineering Department
Bilecik Şeyh Edebali University
Pelitözü Dist. Fatih Sultan Mehmet Boulevard
Gülümbe Campus No:27 11230 BİLECİK / TURKEY
E–mail: ridvan.yayla@bilecik.edu.tr

Emir Albayrak
Computer Engineering Department
Bilecik Şeyh Edebali University
Pelitözü Dist. Fatih Sultan Mehmet Boulevard
Gülümbe Campus No:27 11230 BİLECİK / TURKEY
E–mail: emiralbayrak@gmail.com

Uğur Yüzgeç
Computer Engineering Department
Bilecik Şeyh Edebali University
Pelitözü Dist. Fatih Sultan Mehmet Boulevard
Gülümbe Campus No:27 11230 BİLECİK / TURKEY
E–mail: ugur.yuzgec@bilecik.edu.tr

Identities and generalized derivatives of quasigroups

G. Horosh, N. Malyutina, A. Scerbacova, V. Shcherbacov

Abstract

We associate a partial (autostrophical) identity with every generalized derivative. We research when a quasigroup that satisfies an autostrophic identity has a unit (left or/and right or/and middle).

Keywords: quasigroup, quasigroup derivative, generalized quasigroup derivative, partial identity, right unit, left unit, middle unit.

MSC 2010: 20N05, 68R05.

1 Introduction

This paper is a prolongation of research about units in generalized derivatives of quasigroups started in [14], [16], [20].

Notice, that the biggest part of the results is of combinatorial character, because we have used Prover 9, Mace 4 [17], [18], and standard quasigroup calculations.

Notice, that Prover 9 is one of the best automated reasoning tools and Mace 4 is one of the best constructors of counterexamples. Automated reasoning is the area of computer science that is concerned with applying reasoning in the form of logic to computing systems.

Problem 1 (Belousov's Problem #18 [1]). How to recognize identities which force quasigroups satisfying them to be loops?

The prominent role is played by the newly introduced notion of derivative operation, generalizing Belousov's notions of left/right derivative operations for quasigroups.

©2022 by CSJM; G. Horosh, N. Malyutina, A. Scerbacova, V. Shcherbacov
doi:10.56415/csjm.v30.10

Partial solutions to Belousov's Problem # 18 and their generalizations are obtained.

We would like to remember, that quasigroups have wide applications in cryptology (stream ciphers, cryptcodes, hash functions, secret-sharing schemes, El Gamal signature schemes, etc.) [20].

In order to make reading of this paper more comfortable, we repeat some concepts and definitions from [14].

1.1 Quasigroup

Definition 1. *Garrett Birkhoff [7], [9] has defined an equational quasigroup as an algebra with three binary operations $(Q, \cdot, /, \backslash)$ that satisfies the following six identities:*

$$x \cdot (x\backslash y) = y, \tag{1}$$

$$(y/x) \cdot x = y, \tag{2}$$

$$x\backslash(x \cdot y) = y, \tag{3}$$

$$(y \cdot x)/x = y, \tag{4}$$

$$x/(y\backslash x) = y, \tag{5}$$

$$(x/y)\backslash x = y. \tag{6}$$

Definition 2. *[8], [9], [13]. A groupoid $(Q, \cdot)$ is called a quasigroup if on the set Q there exist operations "$\backslash$" and "$/$" such that in the algebra $(Q, \cdot, \backslash, /)$ identities (1)–(4) are fulfilled.*

1.2 Parastrophes

Definition 3. *An n-ary groupoid (Q, A) with n-ary operation A such that in the equality $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ the fact of knowing any n elements of the set $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ uniquely specifies the remaining one element, is called an n-ary quasigroup [3].*

If we put $n = 2$, then we obtain one more definition of a binary quasigroup.

Definition 4. *From Definition 3 it follows that with a given binary quasigroup* (Q, A) *it is possible to associate* $(3! - 1)$ *other so-called parastrophes of quasigroup* (Q, A)*:*

1. $A(x_1, x_2) = x_3 \Longleftrightarrow$
2. $A^{(12)}(x_2, x_1) = x_3 \Longleftrightarrow$
3. $A^{(13)}(x_3, x_2) = x_1 \Longleftrightarrow$
4. $A^{(23)}(x_1, x_3) = x_2 \Longleftrightarrow$
5. $A^{(123)}(x_2, x_3) = x_1 \Longleftrightarrow$
6. $A^{(132)}(x_3, x_1) = x_2$

[21, p. 230], [1, p. 18], [4].

1.3 Translations

The following table (Table 1) shows for each kind of translation the equivalent one in each of the (six) parastrophes of a quasigroup $(Q, \cdot)$. In fact, Table 1 is a rewritten form of results on three kinds of translations from [2]. See also [12], [19].

Table 1. Translations of quasigroup parastrophes.

	ε	(12)	(13)	(23)	(123)	(132)
R	R	L	R^{-1}	P	P^{-1}	L^{-1}
L	L	R	P^{-1}	L^{-1}	R^{-1}	P
P	P	P^{-1}	L^{-1}	R	L	R^{-1}
R^{-1}	R^{-1}	L^{-1}	R	P^{-1}	P	L
L^{-1}	L^{-1}	R^{-1}	P	L	R	P^{-1}
P^{-1}	P^{-1}	P	L	R^{-1}	L^{-1}	R

From Table 1 it follows, for example, that $R^{(132)} = L^{-1} = L^{(23)} = P^{(13)} = (R^{-1})^{(12)} = (P^{-1})^{(123)}$.

1.4 Unit elements

Suppose we have a quasigroup $(Q, \cdot)$.

Definition 5. *The fact that an element $f \in Q$ is a left identity element (left unit) for quasigroup $(Q, \cdot)$ means that $f \cdot x = x$ for all $x \in Q$.*

The fact that an element $e \in Q$ is a right identity element (right unit) for quasigroup $(Q, \cdot)$ means that $x \cdot e = x$ for all $x \in Q$.

The fact that an element $s \in Q$ is a middle identity element (middle unit) for quasigroup $(Q, \cdot)$ means that $s = x \cdot x$ for all $x \in Q$.

1.5 Generalized derivatives

By the letter T we denote the set of all quasigroup translations of a fixed quasigroup $(Q, \cdot)$ and their inverses relatively one fixed element, say, relatively element a.

Definition 6. *Quasigroup $(Q, \star) = (Q, \cdot)(\alpha, \beta, \gamma)$, where $(Q, \star)$ is isostrophic image of quasigroup $(Q, \cdot)$, i.e., $\cdot \in \{A, A^{(12)}, A^{(13)}, A^{(23)}, A^{(123)}, A^{(132)}\}$, $\alpha, \beta, \gamma \in T$, and in every case one of the translations α, β, γ is an identity permutation, is called an isostrophic (generalized) derivative of quasigroup $(Q, \cdot)$ with respect to element a [14].*

2 Some results

2.1 Autostrophies of quasigroups from generalized derivatives

From Definition 6 it follows the following

Definition 7. *Quasigroup $(Q, \star) = (Q, \cdot)(\alpha, \beta, \gamma)$, where $(Q, \star)$ is one of parastrophes of quasigroup $(Q, \cdot)$, $\alpha, \beta, \gamma \in T$, and in every case one of the translations α, β, γ, is an identity permutation, is called a derivative autostrophy of quasigroup $(Q, \cdot)$ with respect to element a.*

We can name cortege $[(\alpha, \beta, \gamma), (Q, \star)]$ as nuclear autostrophy of a type $(Q, \star)$.

For example, we can name cortege $\left[(L_a, P_a^{-1}, \varepsilon), x\backslash y\right]$ as middle nuclear autostrophy of type $x\backslash y$.

It is clear that a quasigroup can have or cannot have a derivative autostrophy.

As in the case of derivatives which are connected with autotopies, we can look at generalized derivatives

(i) as at autostrophies of quasigroup $(Q, \cdot)$;

(ii) as at identity with some fixed elements [5], [6];

(iii) as at a special nuclear autostrophy [11];

(iv) as at a nuclear identity [11].

All these approaches to derivative autostrophies are presented in [10]. Notice, it is possible to look at derivatives from the point of view

(v) of some functional equations which are defined on quasigroups or on the related groupoids [15].

2.2 Theorems and examples

Theorem 1. *Quasigroup $(Q, \cdot, /, \backslash)$ with autostrophy $((\varepsilon, L_a, R_a), x \cdot y)$ has right unit element (Subtable 15, first row).*

Proof. We can re-write autostrophy $((\varepsilon, L_a, R_a), x \cdot y)$ in the form

$$(x \cdot y) \cdot a = x \cdot (a \cdot y). \tag{7}$$

In equality (7) we substitute the term $x\backslash y$ instead of variable y and obtain

$$(x \cdot (x\backslash y)) \cdot a \overset{(1)}{=} y \cdot a = x \cdot (a \cdot (x\backslash y)). \tag{8}$$

i.e.,

$$y \cdot a = x \cdot (a \cdot (x\backslash y)). \tag{9}$$

Further, we multiply both sides of equality (9) from the left by the term $x\backslash t$ and, using identity (3), we obtain

$$x\backslash(y \cdot a) = x\backslash(x \cdot (a \cdot (x\backslash y))) \overset{(3)}{=} a \cdot (x\backslash y), \tag{10}$$

i.e.,

$$x\backslash(y \cdot a) = a \cdot (x\backslash y). \tag{11}$$

If we put $x = y$ in equality (11), then we obtain

$$x\backslash(x \cdot a) \overset{(3)}{=} a = a \cdot (x\backslash x). \tag{12}$$

From equality (12), we have

$$x\backslash x = a\backslash a \tag{13}$$

and finally, we have

$$x \cdot (a\backslash a) = x. \tag{14}$$

□

Example 1. *We demonstrate that quasigroup $(Q, \cdot, /, \backslash)$ with partial identity (7) has no left and middle unit.*

$\cdot$	0	1	2	3	4	5
0	1	0	4	5	2	3
1	0	1	3	2	5	4
2	4	2	5	1	3	0
3	5	3	2	0	4	1
4	2	4	0	3	1	5
5	3	5	1	4	0	2

Example 2. *The cortege $\left[(L_a, P_a^{-1}, \varepsilon), x\backslash y\right]$ means autostrophy of the form: $L_a x \cdot P_a^{-1} y = x\backslash y$.*

Using table of translations (Table 1), we can re-write the last equality in the following form:

$$(a \cdot x) \cdot (a/y) = x\backslash y. \tag{15}$$

We have an identity of two variables and one fixed element on quasigroup $(Q, \cdot, /, \backslash)$.

From Table 2, it follows that quasigroup $(Q, \cdot)$ with equality (15) has no left (right, middle) identity element, i.e., it is a constructed quasigroup $(Q, \cdot, /, \backslash)$ with partial identity (15) which has no left (right, middle) identity element for some fixed element a. We give the needed example:

$\cdot$	0	1	2	3	4
0	1	3	0	2	4
1	3	0	2	4	1
2	0	2	4	1	3
3	2	4	1	3	0
4	4	1	3	0	2

Example 3. *The cortege* $\left[(\varepsilon, P_a^{-1}, P_a), xy\right]$ *means the following autostrophy (autostrophic derivative) of quasigroup* $(Q, \cdot)$*:* $x \cdot P_a^{-1} y = P_a(xy)$.

Using Table 1, we can re-write the last equality in the following form:

$$(xy)\backslash a = x \cdot (a/y). \tag{16}$$

From Table 2, it follows that quasigroup with equality (16) has middle identity element (see Theorem 2) and has no left and right identity element. See counterexample below. In this counterexample $a = 0$.

$\cdot$	0	1	2	3
0	1	0	2	3
1	0	1	3	2
2	2	3	1	0
3	3	2	0	1

Theorem 2. *Quasigroup* $(Q, \cdot, /, \backslash)$ *with partial identity (16) has middle identity element.*

Proof. From equality (16), substituting $x\backslash y$ instead of y, we have

$$(x \cdot (x\backslash y))\backslash a \overset{(1)}{=} y\backslash a = x \cdot (a/(x\backslash y)). \tag{17}$$

If we substitute $y = a$ in (17), then we have

$$a\backslash a = x \cdot (a/(x\backslash a)) \overset{(5)}{=} x \cdot x \tag{18}$$

for all $x \in Q$. Then $x \cdot x = a\backslash a$ for all $x \in Q$. □

In Table 2, the cortege $[(L_a, L_a, \varepsilon), x/y]$ means the following autostrophy of quasigroup $(Q, \cdot)$: $L_a x \cdot L_a y = x/y$.

Using table of translations (Table 1), we can re-write the last equality in the following form:

$$(a \cdot x) \cdot (a \cdot y) = x/y. \tag{19}$$

Theorem 3. *Quasigroup $(Q, \cdot, /, \backslash)$ with identity (19) has left and middle identity element.*

Proof. Firstly, we prove that any quasigroup with this partial identity has the left identity element. We substitute term $y\backslash x$ in identity (19) for variable y. We have

$$(a \cdot x) \cdot (a \cdot (y\backslash x)) = x/(y\backslash x) \overset{(5)}{=} y. \tag{20}$$

We substitute term xy in identity (19) for variable x. We have

$$(a \cdot xy) \cdot (ay) = (xy)/y \overset{(4)}{=} x. \tag{21}$$

If we substitute $y = a$ in equality (20), then we have

$$(a \cdot x) \cdot (a \cdot (a\backslash x)) = a. \tag{22}$$

But by identity (4), $a \cdot (a\backslash x) = x$. Therefore,

$$(a \cdot x) \cdot x = a. \tag{23}$$

If in equality (23) we substitute term $a\backslash x$ for variable x, we have

$$(a \cdot (a\backslash x)) \cdot (a\backslash x) = a. \tag{24}$$

Taking into consideration that $a \cdot (a\backslash x) \overset{(1)}{=} x$, further we have

$$x \cdot (a\backslash x) = a. \tag{25}$$

If we substitute the term $a\backslash x$ for variable y in equality (21), then we have

$$(a \cdot x(a\backslash x)) \cdot (a(a\backslash x)) = x. \tag{26}$$

If we apply equalities (25) $(x(a\backslash x) = a)$ and identity (1) to the left part of the last equality, then we obtain

$$(a \cdot a) \cdot x = x, \tag{27}$$

i.e., quasigroup with identity (19) has left identity element.

Secondly. We prove that this quasigroup has middle unit element. We denote element $a \cdot a$ as the left unit f. In the equality (21), we substitute $x = f$ and we obtain

$$(ay)(ay) = f. \tag{28}$$

If in the equality (28) we substitute the term $a\backslash y$ for the variable y, then we have

$$yy = f. \tag{29}$$

Therefore, quasigroup with identity (19) has the middle unit. □

Example 4. *The following example demonstrates that quasigroup with identity (19) cannot have the right unit.*

$\cdot$	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	2	3	1	0
3	3	2	0	1

Here $a = 0$.

Example 5. *In Table 2 (Subtable 107, row 5), the cortege* $\left[(\varepsilon, P_a^{-1}, P_a), y/x\right]$ *means the following autostrophy of quasigroup* $(Q, \cdot)$*:* $x \cdot P_a^{-1}y = P_a(y/x)$*. Using table of translations (Table 1), we can rewrite the last equality in the following form:* $(y/x)\backslash a = x \cdot (a/y)$.

From Table 2, it follows that if quasigroup $(Q, \cdot, /, \backslash)$ *has the autostrophy* $\left[(\varepsilon, P_a^{-1}, P_a), y/x\right]$*, then quasigroup* $(Q, \cdot)$ *has right unit (see Theorem 4), and in general, this quasigroup cannot have left and middle unit (see counter-example below).*

$\cdot$	0	1	2	3
0	0	2	3	1
1	1	3	2	0
2	2	0	1	3
3	3	1	0	2

Theorem 4. *Quasigroup $(Q, \cdot, /, \backslash)$ with partial identity*

$$(y/x)\backslash a = x \cdot (a/y) \tag{30}$$

has right unit.

Proof. We substitute $y = a$ in partial identity (30) and we have

$$(a/x)\backslash a \overset{(6)}{=} x = x \cdot (a/a). \tag{31}$$

From identity (31), we have that $x = x \cdot (a/a)$, i.e., element (a/a) is a right unit in quasigroup $(Q, \cdot, /, \backslash)$.

□

Example 6. *We can re-write autostrophy $[(\varepsilon, P_a^{-1}, P_a^{-1}), y/x]$ (Subtable 108, 5 row) in the following form*

$$x \cdot (a/y) = a/(y/x). \tag{32}$$

We demonstrate that quasigroup $(Q, \cdot, /, \backslash)$ has no left, right and middle unit element.

$\cdot$	0	1	2	3	4	5
0	1	0	4	5	2	3
1	0	1	3	2	5	4
2	5	3	2	1	4	0
3	4	2	1	3	0	5
4	3	5	0	4	1	2
5	2	4	5	0	3	1

2.3 Table

We collect the obtained results in the following Table 2.

When filling out Table 2, we have used Prover 9, Mace 4 [17], [18] and standard quasigroup calculations.

In fact, Table 2 contains formulations of 1944 Theorems and counterexamples about the existence of units (left, right, middle) in quasigroups with identities that are obtained from the generalized derivatives of a quasigroup $(Q, \cdot, /, \backslash)$.

For every case a theorem is proved (usually by Prover) or there is constructed a counterexample (usually by Mace). Every sign "+"means that quasigroup with respective autostrophy (partial identity) has a corresponding unit element.

In the next papers, we plan to give human proof for the largest part of the theorems.

Table 2: Units in quasigroup that is a generalized derivative.

Avtstr.	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**
$1.(L_a, L_a, \varepsilon)$	f	e	s	$2.(L_a, L_a^{-1}, \varepsilon)$	f	e	s	$3.(L_a, R_a, \varepsilon)$	f	e	s
xy	+	-	-	xy	+	-	-	xy	-	-	-
yx	-	+	-	yx	-	+	-	yx	+	+	-
$x\backslash y$	-	-	-	$x\backslash y$	+	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	+	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	+	-	+	x/y	-	-	+	x/y	-	-	-
$4.(L_a, R_a^{-1}, \varepsilon)$	f	e	s	$5.(L_a, P_a, \varepsilon)$	f	e	s	$6.(L_a, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	-	-	xy	+	-	-	xy	+	-	-
yx	-	+	-	yx	-	+	-	yx	-	+	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	+	-	-	$y\backslash x$	-	-	-
y/x	+	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	+	-	-
$7.(L_a, \varepsilon, L_a)$	f	e	s	$8.(L_a, \varepsilon, L_a^{-1})$	f	e	s	$9.(L_a, \varepsilon, R_a)$	f	e	s
xy	+	-	-	xy	+	-	-	xy	+	-	-
yx	+	+	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	+	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	+	+	y/x	-	-	+	y/x	+	-	+
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-
$10.(L_a, \varepsilon, R_a^{-1})$	f	e	s	$11.(L_a, \varepsilon, P_a)$	f	e	s	$12.(L_a, \varepsilon, P_a^{-1})$	f	e	s
xy	+	-	-	xy	-	-	-	xy	-	-	-
yx	+	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	+	y/x	-	-	+	y/x	-	-	+
x/y	-	-	-	x/y	+	-	-	x/y	-	-	-
$13.(\varepsilon, L_a, L_a)$	f	e	s	$14.(\varepsilon, L_a, L_a^{-1})$	f	e	s	$15.(\varepsilon, L_a, R_a)$	f	e	s
xy	-	-	-	xy	-	-	-	xy	-	+	-
yx	+	+	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	+
$y\backslash x$	-	+	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-	-	-	y/x	-	-	+
x/y	+	-	+	x/y	-	-	+	x/y	-	+	+
$16.(\varepsilon, L_a, R_a^{-1})$	f	e	s	$17.(\varepsilon, L_a, P_a)$	f	e	s	$18.(\varepsilon, L_a, P_a^{-1})$	f	e	s
xy	-	+	-	xy	-	-	+	xy	-	-	+
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	+	x/y	-	-	+	x/y	-	-	+
19. $(L_a^{-1}, L_a, \varepsilon)$	f	e	s	20. $(L_a^{-1}, L_a^{-1}, \varepsilon)$	f	e	s	21. $(L_a^{-1}, R_a, \varepsilon)$	f	e	s
xy	+	-	-	xy	+	-	-	xy	-	-	-
yx	-	-	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	+	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	+	-	$y\backslash x$	-	+	+	$y\backslash x$	-	+	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-

Continued on next page

Table 2 – *Continued from previous page*

Avtstr.	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**
x/y	-	-	-	x/y	+	-	+	x/y	-	-	-
22. $(L_a^{-1}, R_a^{-1}, \varepsilon)$	f	e	s	23. $(L_a^{-1}, P_a, \varepsilon)$	f	e	s	24. $(L_a^{-1}, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	-	-	xy	+	-	-	xy	+	-	-
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	+	-	$y\backslash x$	+	+	-	$y\backslash x$	-	+	-
y/x	+	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	+	-	-
25. $(L_a^{-1}, \varepsilon, L_a)$	f	e	s	26. $(L_a^{-1}, \varepsilon, L_a^{-1})$	f	e	s	27. $(L_a^{-1}, \varepsilon, R_a)$	f	e	s
xy	+	-	-	xy	+	-	-	xy	+	-	-
yx	-	+	-	yx	+	+	-	yx	-	-	-
$x\backslash y$	+	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	+	-	y/x	-	-	-	y/x	+	-	-
x/y	-	-	+	x/y	-	-	+	x/y	-	-	+
28. $(L_a^{-1}, \varepsilon, R_a^{-1})$	f	e	s	29. $(L_a^{-1}, \varepsilon, P_a)$	f	e	s	30. $(L_a^{-1}, \varepsilon, P_a^{-1})$	f	e	s
xy	+	-	-	xy	-	-	-	xy	-	-	-
yx	+	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-		-	y/x	-	-	-
x/y	-	-	+	x/y	+	-	+	x/y	-	-	+
31.$(\varepsilon, L_a^{-1}, L_a)$	f	e	s	32$(\varepsilon, L_a^{-1}, L_a^{-1})$	f	e	s	33.$(\varepsilon, L_a^{-1}, R_a)$	f	e	s
xy	-	-	-	xy	-	-	-	xy	-	+	-
yx	-	-	-	yx	+	+	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	+
$y\backslash x$	-	+	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	+	y/x	-	-	+	y/x	-	-	+
x/y	-	-	-	x/y	+	-	+	x/y	-	+	-
34. $(\varepsilon, L_a^{-1}, R_a^{-1})$	f	e	s	35. $(\varepsilon, L_a^{-1}, P_a)$	f	e	s	36. $(\varepsilon, L_a^{-1}, P_a^{-1})$	f	e	s
xy	-	+	-	xy	-	-	+	xy	-	-	+
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	-	+	y/x	-	+	+	y/x	-	-	+
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-
37.(R_a, L_a, ε)	f	e	s	38.$(R_a, L_a^{-1}, \varepsilon)$	f	e	s	39.(R_a, R_a, ε)	f	e	s
xy	+	+	-	xy	+	+	-	xy	-	+	-
yx	-	-	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	+	-	-	$x\backslash y$	-	+	+
$y\backslash x$	-	-	-	$y\backslash x$	-	-	+	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	+	x/y	-	-	-
40.$(R_a, R_a^{-1}, \varepsilon)$	f	e	s	41.(R_a, P_a, ε)	f	e	s	42.$(R_a, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	+	-	xy	-	+	-	xy	-	+	-
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	+	-	-	$y\backslash x$	-	-	-
y/x	+	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	+	-	-
43.(R_a, ε, L_a)	f	e	s	44.$(R_a, \varepsilon, L_a^{-1})$	f	e	s	45.(R_a, ε, R_a)	f	e	s
xy	+	-	-	xy	+	-	-	xy	-	-	-
yx	-	+	-	yx	-	-	-	yx	+	+	-
$x\backslash y$	+	-	+	$x\backslash y$	-	-	+	$x\backslash y$	-	+	+
$y\backslash x$	-	-	+	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	+	-	y/x	-	-	-	y/x	+	-	-
x/y	-	-	+	x/y	-	-	-	x/y	-	-	-
46.$(R_a, \varepsilon, R_a^{-1})$	f	e	s	47.(R_a, ε, P_a)	f	e	s	48.$(R_a, \varepsilon, P_a^{-1})$	f	e	s

Continued on next page

Table 2 – *Continued from previous page*

Avtstr.	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**
xy	-	-	-	xy	-	-	+	xy	-	-	+
yx	+	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	+	$x\backslash y$	-	-	+	$x\backslash y$	-	-	+
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	+	-	-	x/y	-	-	-

49.(ε, R_a, L_a)	f	e	s	50.$(\varepsilon, R_a, L_a^{-1})$	f	e	s	51.(ε, R_a, R_a)	f	e	s
xy	-	+	-	xy	-	+	-	xy	-	+	-
yx	-	-	-	yx	-	+	-	yx	+	+	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	+
$y\backslash x$	-	+	+	$y\backslash x$	-	-	+	$y\backslash x$	+	-	+
y/x	-	-	-	y/x	-	-	-	y/x	-	-	+
x/y	-	-	-	x/y	-	-	-	x/y	-	+	-
52.$(\varepsilon, R_a, R_a^{-1})$	f	e	s	53.(ε, R_a, P_a)	f	e	s	54.$(\varepsilon, R_a, P_a^{-1})$	f	e	s
xy	-	+	-	xy	-	-	-	xy	-	-	-
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	+	$y\backslash x$	-	-	+
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-

55. $(R_a^{-1}, L_a, \varepsilon)$	f	e	s	56. $(R_a^{-1}, L_a^{-1}, \varepsilon)$	f	e	s	57. $(R_a^{-1}, R_a, \varepsilon)$	f	e	s
xy	+	+	-	xy	+	+	-	xy	-	+	-
yx	+	-	-	yx	+	+	-	yx	+	-	-
$x\backslash y$	-	-	+	$x\backslash y$	+	-	+	$x\backslash y$	-	-	+
$y\backslash x$	+	-	-	$y\backslash x$	+	-	+	$y\backslash x$	+	-	-
y/x	-	-	+	y/x	-	+	+	y/x	-	-	+
x/y	-	+	-	x/y	-	+	+	x/y	-	+	-
58. $(R_a^{-1}, R_a^{-1}, \varepsilon)$	f	e	s	59. $(R_a^{-1}, P_a, \varepsilon)$	f	e	s	60. $(R_a^{-1}, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	+	-	xy	-	+	-	xy	-	+	-
yx	+	-	-	yx	+	-	-	yx	+	-	-
$x\backslash y$	-	+	+	$x\backslash y$	-	-	+	$x\backslash y$	-	-	+
$y\backslash x$	+	-	-	$y\backslash x$	+	-	-	$y\backslash x$	+	-	-
y/x	+	-	+	y/x	-	-	+	y/x	-	-	+
x/y	-	+	-	x/y	-	+	-	x/y	+	+	-

61.$(R_a^{-1}, \varepsilon, L_a)$	f	e	s	62$(R_a^{-1}, \varepsilon, L_a^{-1})$	f	e	s	63.$(R_a^{-1}, \varepsilon, R_a)$	f	e	s
xy	+	-	-	xy	+	-	-	xy	-	-	-
yx	-	+	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	+	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	+	$y\backslash x$	-	-	+
y/x	-	+	-	y/x	-	-	-	y/x	+	-	-
x/y	-	-	+	x/y	-	-	-	x/y	-	-	-
64. $(R_a^{-1}, \varepsilon, R_a^{-1})$	f	e	s	65. $(R_a^{-1}, \varepsilon, P_a)$	f	e	s	66. $(R_a^{-1}, \varepsilon, P_a^{-1})$	f	e	s
xy	-	-	-	xy	-	-	+	xy	-	-	+
yx	+	+	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	+	+	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	+	$y\backslash x$	+	-	+
y/x	-	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	+	-	-	x/y	-	-	-

67. $(\varepsilon, R_a^{-1}, L_a)$	f	e	s	68. $(\varepsilon, R_a^{-1}, L_a^{-1})$	f	e	s	69. $(\varepsilon, R_a^{-1}, R_a)$	f	e	s
xy	-	+	-	xy	-	+	-	xy	-	+	-
yx	-	-	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	-	+	$x\backslash y$	-	-	+	$x\backslash y$	-	-	+
$y\backslash x$	-	+	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-	-	-	y/x	-	-	+
x/y	-	-	-	x/y	-	-	-	x/y	-	+	-
70. $(\varepsilon, R_a^{-1}, R_a^{-1})$	f	e	s	71. $(\varepsilon, R_a^{-1}, P_a)$	f	e	s	72. $(\varepsilon, R_a^{-1}, P_a^{-1})$	f	e	s
xy	-	+	-	xy	-	-	-	xy	-	-	-

Continued on next page

Table 2 – *Continued from previous page*

Avtstr.	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**
yx	+	+	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	+	$x\backslash y$	-	-	+	$x\backslash y$	-	+	+
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-
73.(P_a, L_a, ε)	f	e	s	74.$(P_a, L_a^{-1}, \varepsilon)$	f	e	s	75.(P_a, R_a, ε)	f	e	s
xy	+	-	-	xy	+	-	-	xy	-	+	-
yx	-	-	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	+	-	$x\backslash y$	+	+	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	+	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	+	x/y	-	-	-
76.$(P_a, R_a^{-1}, \varepsilon)$	f	e	s	77.(P_a, P_a, ε)	f	e	s	78.$(P_a, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	+	-	xy	-	-	-	xy	-	-	-
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	+	-	$x\backslash y$	-	+	+	$x\backslash y$	-	+	-
$y\backslash x$	-	+	-	$y\backslash x$	+	-	-	$y\backslash x$	-	-	-
y/x	+	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	+	-	-
79.(P_a, ε, L_a)	f	e	s	80.$(P_a, \varepsilon, L_a^{-1})$	f	e	s	81.(P_a, ε, R_a)	f	e	s
xy	+	-	+	xy	+	-	+	xy	-	-	+
yx	-	+	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	+	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	+	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	+	-	y/x	-	-	-	y/x	+	-	-
x/y	-	-	+	x/y	-	-	-	x/y	-	-	-
82.$(P_a, \varepsilon, R_a^{-1})$	f	e	s	83.(P_a, ε, P_a)	f	e	s	84.$(P_a, \varepsilon, P_a^{-1})$	f	e	s
xy	-	-	+	xy	-	-	+	xy	-	-	+
yx	+	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-	-	-	y/x	-	-	-
x/y	-	-	-	x/y	+	-	-	x/y	-	-	-
85.(ε, P_a, L_a)	f	e	s	86.$(\varepsilon, P_a, L_a^{-1})$	f	e	s	87.(ε, P_a, R_a)	f	e	s
xy	-	-	+	xy	-	-	+	xy	-	+	+
yx	-	-	+	yx	-	+	+	yx	+	-	+
$x\backslash y$	-	+	-	$x\backslash y$	-	+	-	$x\backslash y$	-	+	+
$y\backslash x$	-	+	-	$y\backslash x$	-	+	-	$y\backslash x$	+	+	-
y/x	+	-	-	y/x	+	-	-	y/x	+	-	+
x/y	+	-	-	x/y	+	-	-	x/y	+	+	-
88.$(\varepsilon, P_a, R_a^{-1})$	f	e	s	89.(ε, P_a, P_a)	f	e	s	90.$(\varepsilon, P_a, P_a^{-1})$	f	e	s
xy	-	+	-	xy	-	-	-	xy	-	-	-
yx	-	-	+	yx	-	-	+	yx	-	-	+
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-
91. $(P_a^{-1}, L_a, \varepsilon)$	f	e	s	92. $(P_a^{-1}, L_a^{-1}, \varepsilon)$	f	e	s	93. $(P_a^{-1}, R_a, \varepsilon)$	f	e	s
xy	+	-	-	xy	-	-	-	xy	-	-	-
yx	-	-	-	yx	-	-	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	+	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	+	-	y/x	-	+	-	y/x	-	+	-
x/y	-	-	-	x/y	-	-	-	x/y	-	-	-
94. $(P_a^{-1}, R_a^{-1}, \varepsilon)$	f	e	s	95. $(P_a^{-1}, P_a, \varepsilon)$	f	e	s	96. $(P_a^{-1}, P_a^{-1}, \varepsilon)$	f	e	s
xy	-	-	-	xy	-	-	-	xy	-	-	-
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	-
$y\backslash x$	-	-	-	$y\backslash x$	+	-	-	$y\backslash x$	-	-	-
y/x	+	+	-	y/x	-	+	-	y/x	-	+	-

Continued on next page

Table 2 – *Continued from previous page*

Avtstr.	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**	**Avtstr.**	**f**	**e**	**s**
x/y	-	-	-	x/y	-	-	-	x/y	+	-	-
97. $(P_a^{-1}, \varepsilon, L_a)$	f	e	s	98. $(P_a^{-1}, \varepsilon, L_a^{-1})$	f	e	s	99. $(P_a^{-1}, \varepsilon, R_a)$	f	e	s
xy	+	-	+	xy	+	-	+	xy	-	-	+
yx	-	+	+	yx	-	-	+	yx	-	-	+
$x\backslash y$	+	+	-	$x\backslash y$	-	+	-	$x\backslash y$	-	+	-
$y\backslash x$	-	+	+	$y\backslash x$	-	+	-	$y\backslash x$	-	+	-
y/x	+	+	-	y/x	+	-	-	y/x	+	-	-
x/y	+	-	+	x/y	+	-	-	x/y	+	-	-
100. $(P_a^{-1}, \varepsilon, R_a^{-1})$	f	e	s	101. $(P_a^{-1}, \varepsilon, P_a)$	f	e	s	102. $(P_a^{-1}, \varepsilon, P_a^{-1})$	f	e	s
xy	-	-	+	xy	-	-	+	xy	-	-	+
yx	+	-	+	yx	-	-	+	yx	-	-	+
$x\backslash y$	-	+	-	$x\backslash y$	-	+	-	$x\backslash y$	-	+	+
$y\backslash x$	-	+	-	$y\backslash x$	-	+	-	$y\backslash x$	+	+	-
y/x	+	-	-	y/x	+	-	-	y/x	+	-	+
x/y	+	-	-	x/y	+	-	-	x/y	+	-	-
103. $(\varepsilon, P_a^{-1}, L_a)$	f	e	s	104. $(\varepsilon, P_a^{-1}, L_a^{-1})$	f	e	s	105. $(\varepsilon, P_a^{-1}, R_a)$	f	e	s
xy	-	-	+	xy	-	-	+	xy	-	+	+
yx	-	-	-	yx	-	+	-	yx	+	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	-	+
$y\backslash x$	-	+	-	$y\backslash x$	-	-	-	$y\backslash x$	+	-	-
y/x	-	-	-	y/x	-	-	-	y/x	-	-	+
x/y	-	-	-	x/y	-	-	-	x/y	-	+	-
106. $(\varepsilon, P_a^{-1}, R_a^{-1})$	f	e	s	107. $(\varepsilon, P_a^{-1}, P_a)$	f	e	s	108. $(\varepsilon, P_a^{-1}, P_a^{-1})$	f	e	s
xy	-	+	+	xy	-	-	+	xy	-	-	+
yx	-	-	-	yx	-	-	-	yx	-	-	-
$x\backslash y$	-	-	-	$x\backslash y$	-	-	-	$x\backslash y$	-	+	-
$y\backslash x$	-	-	-	$y\backslash x$	-	-	-	$y\backslash x$	-	-	-
y/x	-	-	-	y/x	-	+	-	y/x	-	-	-
x/y	-	-	-	x/y	-	-	-	x/y	+	-	+

References

[1] V.D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Moscow: Nauka, 1967. (in Russian).

[2] V.D. Belousov, "On a group associated with a quasigroup," *Mat. Issled.*, vol. 4, no. 3, pp. 27–39, 1969. (in Russian).

[3] V.D. Belousov, *n-Ary Quasigroups*, Kishinev: Stiintsa, 1971. (in Russian).

[4] V.D. Belousov, *Elements of Quasigroup Theory: a Special Course*, Kishinev: Kishinev State University Printing House, 1981. (in Russian).

[5] V.D. Belousov and A.A. Gvaramiya, "Partial identities and nuclei of quasigroups," *Bulletin of the Academy of Sciences of the Georgian SSR*, vol. 65, no. 2, pp. 277–279, 1972. (in Russian).

[6] G.B. Belyavskaya, "Identities with permutations and quasigroups isotopic to groups and abelian groups," *Discret. Mat.*, vol. 25, no. 2, pp. 68–81, 2013. (Russian).

[7] G. Birkhoff, *Lattice Theory (American Mathematical Society Colloquium Publications)*, Revised edition, vol. 25, New York: American Mathematical Society, 1948.

[8] G. Birkhoff, *Lattice Theory (American Mathematical Society Colloquium Publications, vol. XXV)*, Third edition, American Mathematical Society, 1967.

[9] G. Birkhoff, *Lattice Theory*, Moscow: Nauka, 1984. (Russian translation).

[10] Natalia N. Didurik and Victor A. Shcherbacov, "Units in quasigroups with Bol-Moufang type identities," Presentation, July 2019. Available: https://algebra.math.bme.hu/LOOPS19/slides/shcerbacov.pdf.

[11] A. Drapal and P. Jedlička, "On loop identities that can be obtained by a nuclear identification," 2007. [Online]. Available: http://tf.czu.cz/ jedlickap/a/2007nucid.pdf.

[12] J. Duplak, "A parastrophic equivalence in quasigroups," *Quasigroups Relat. Syst.*, vol. 7, pp. 7–14, 2000.

[13] T. Evans, "Homomorphisms of non-associative systems," *J. London Math. Soc.*, vol. 24, pp. 254–260, 1949.

[14] G. Horosh, N. Malyutina, A. Scerbacova, and V. Shcherbacov, "Units in generalized derivatives of quasigroups," 2020. arXiv: 2009.03605.

[15] A. Krapez, "Weak Associativity and Quasigroup Units," *Publ. Inst. Math.*, vol. 105, pp. 17–24, 2019.

[16] A. Krapez and V. A. Shcherbacov, "Quasigroups, Units and Belousov's Problem # 18," *Armen. J. Math.*, vol. 11, no. 9, pp. 1–27, 2019.

[17] W. McCune, *Mace 4,* University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

[18] W. McCune, *Prover 9*, University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

[19] V.A. Shcherbacov, "On definitions of groupoids closely connected with quasigroups," *Bul. Acad. Stiinte Repub. Mold., Mat.*, no. 2(54), pp. 43–54, 2007.

[20] Victor Shcherbacov, *Elements of Quasigroup Theory and Applications*, Boca Raton: CRC Press, 2017.

[21] Sh. K. Stein, "On the foundations of quasigroups," *Trans. Amer. Math. Soc.*, vol. 85, no. 1, pp. 228–256, 1957.

Grigorii Horosh[1], Nadeghda Malyutina[2],
Alexandra Scerbacova[3], Victor Shcherbacov[4]

Received March 9, 2022
Accepted May 6, 2022

[1]Ph.D. Student
Moldova State University
E–mail: grigorii.horos@math.md

[2]Ph.D. Student
Moldova State University
E–mail: 231003.bab.nadezhda@mail.ru

[3]Ph.D. Student
Skolkovo Institute of Science and Technology
E–mail: scerbik33@yandex.ru

[4]Principal Researcher
Vladimir Andrunachievici Institute of Mathematics and
Computer Science of Moldova
E–mail: victor.scerbacov@math.md

Degree of favoring in apportionments

Ion Bolun

Abstract

To quantitatively estimate the degree of favoring the beneficiaries in proportional apportionments of entities of the same kind (seats, PCs, etc.), five quantitative criteria were defined. By computer simulation, the degree of favoring the large or small beneficiaries by 6 apportionment methods is identified. Thus, favoring large beneficiaries by the d'Hondt method can overpass 10.7-12.1 entities (entities in excess) and that of small beneficiaries by the Huntington-Hill method – 2.7-11.0 entities, and by the Adapted Sainte-Laguë method – 1.7-9.7 entities. The Huntington-Hill method favors small beneficiaries up to 5.70 times stronger than the Adapted Sainte-Laguë one does. Also, the d'Hondt method favors beneficiaries (the large ones) much stronger than the Adapted Sainte-Laguë one does (the small ones) – for very many cases the respective ratio exceeds 10 times.

Keywords: apportionment method, comparative analysis, computer simulation, criteria, favoring large beneficiaries, favoring small beneficiaries.

MSC 2020: 62P25, 90B50, 91B12

1 Introduction

Often it is necessary to distribute a given number M of discrete entities of the same kind (a-entities) among n beneficiaries (parties, schools, hospitals, etc.) in proportion to a numerical characteristic assigned to each of them $V_i, i = \overline{1,n}$. For example, M may be the total number of seats in the elective body, n – the total number of parties and V – the total number of voters (deciders). This is known as proportional apportionment (APP) problem [1-3]. The integer character of

©2022 by CSJM; Ion Bolun
doi:10.56415/csjm.v30.11

this problem usually causes a certain disproportion of the apportionment $\{x_i, i = \overline{1,n}\}$ [1, 4 - 6], some beneficiaries being favored at the expense of the others (notations $\{c_i, i = \overline{1,n}\}$ and $\{c_1, c_2, ..., c_n\}$ are used equivalently to specify the group of elements $c_1, c_2, ..., c_n$). Such favoring leads to the increase of disproportionality of the apportionment. Therefore, reducing the favoring in question is one of the basic requirements (free of bias condition [1, 3]) when the APP method is chosen to be applied under concrete situations.

As it is well known, the d'Hondt method [7] favors large beneficiaries (with larger V_i value) [1, 4, 8, 9], and Huntington-Hill method [10] favors the small ones (with smaller V_i value) [1, 8]. But which of the two favors beneficiaries to a larger extent? Preferences, in this sense, between methods, can help. For example, in [8], five divisor APP methods are placed "in the order as they are known to favor larger parties over smaller parties: Adams, Dean, Hill, Webster, and Jefferson" (in the increasing order of favoring). However, the best way is to estimate this property quantitatively – the degree of favoring the beneficiaries. Three such approaches are proposed in [12, 13]. These and other approaches, including new criteria for estimating the degree of favoring the large or, on the contrary, the small beneficiaries by APP methods, are explored in this paper by computer simulation.

2 Approaches of favoring in apportionments

The essence of favoring the beneficiaries in apportionments is described in different papers, including [1, 4, 8, 11]. Four such approaches are described below in this section.

Approach 1. Let's consider a-entities as seats, deciders as population and beneficiaries as states. Then, according to [12], "An apportionment that gives x_1 and x_2 seats to states having populations $V_1 > V_2 > 0$ favors the larger state over the smaller state if $x_1/V_1 > x_2/V_2$, and favors the smaller state over the larger state if $x_1/V_1 < x_2/V_2$". To compare APP methods with reference to favoring the states, the bias ratio $\delta/(\gamma + \delta)$ as criterion is proposed; here δ is the number of pairs of states in which the small state is favored and γ is the number of pairs of states in which the large state is fa-

vored. Using this criteria, the results obtained in [12] for the 19 United States Congressional apportionments of seats in the period of 1790-1970 years are (for five APP methods): J.O.Adams – 0.780; J.Dean – 0.583; E.V.Huntington – 0.562; D.Webster – 0.518 and T.Jefferson – 0.199. APP methods are listed in the decreasing order of the bias ratio of favoring the small states, that is in the increasing order of favoring the large states.

Approach 2 [12]. Let g be a number satisfying $x_i > g$ for at least $\lfloor n/2 \rfloor$ states and $x_i < g$ for at least $\lfloor n/2 \rfloor$ states. Define the set of large states as $L = \{i, x_i > g\}$ and the set of small states as $S = \{i, x_i < g\}$; a state with g seats belongs to both L and S. Then, in an apportionment, the large states are favored if $\Sigma_L x_i/\Sigma_L V_i > \Sigma_S x_i/\Sigma_S V_i$ and the small states are favored if $\Sigma_L x_i/\Sigma_L V_i < \Sigma_S x_i/\Sigma_S V_i$. Applying this criterion to the mentioned above 19 apportionments of seats, in [12], the following results are obtained (number of times small states were favored for each of the five APP methods): J.O.Adams – 19; J.Dean – 14; E.V.Huntington – 13; D.Webster – 9, and T.Jefferson – 0. This order of APP methods coincides with the one obtained in Approach 1.

Approach 3. The same order for the five APP methods, but applying an analytical not experimental approach, is obtained in [8, 11]. The type of ordering used is called majorization (majorization ordering). "It has the advantage of providing a complete characterization, and has its roots in studies of equality and inequality" [8, p. 886] and its formal properties [15]. Majorization provides an ordering between two vectors $\mathbf{m} = (m_1, \ldots, m_l)$ and $\mathbf{m'} = (m'_1, \ldots, m'_l)$, with ordered elements $m_1 \geq \ldots, \geq m_l$ and $m'_1 \geq \ldots \geq m'_l$, and with an identical component sum $m_1 + \ldots, + m_l = m'_1 + \ldots + m'_l = M$. The ordering states that all partial sums of the k largest components in $\mathbf{m}$ are dominated by the sum of the k largest components in $\mathbf{m'}$: $m_1 \leq m'_1$, $m_1 + m_2 \leq m'_1 + m'_2, \ldots, m_1 + \ldots, + m_l \leq m'_1 + \ldots + m'_l$.

To compare APP methods by majorization ordering, the notion of majorization from apportionment vectors to apportionment methods is extended and the signpost sequences that determine the methods are used. So [1], a divisor method of apportionment is defined through numbers $s(k)$ in the interval $[k; k+1]$ such that the sequence

$s(0), s(1), ...$ is strictly increasing; here a number $s(k)$ is a "signpost" ("dividing point") splitting the interval $[k; k+1]$ into a left part, where numbers are rounded down to k, and a right part, where numbers are rounded up to $k+1$. For $s(k)$ itself, there is the option to round down to k or to round up to $k+1$, thus possibly generating multiplicities. The numbers rounded this way are the quotients of the weights (V_i) and a divisor (d), $V_1/d, \ldots, V_l/d$, for some choice of divisor $d > 0$ common to all weights. If party i gets m_i seats, then necessarily $s(m_i–1) \leq V_i/d \leq s(m_i)$. The divisor d is adjusted so that the sum of all seats becomes equal to M.

Taking into account the introduced notions, in [8, 11] it is proved that divisor method A is majorized by divisor method A', in sense of favoring, if and only if the ratio $s(k)/s'(k)$ is strictly increasing in k, where $s(k)$ and $s'(k)$ are the signposts for methods A and A', respectively. Finally, it is proved that the divisor method with power-mean rounding of order p is majorized by the divisor method with power-mean rounding of order p' if and only if $p \leq p'$. This statement puts the mentioned above five divisor methods into the majorization ordering that coincides with the one obtained in Approaches 1 and 2.

Approach 4. A more strong, than the three described above approaches, is the one proposed in [1]: an apportionment method favors large parties if $\Sigma_L x_i/\Sigma_L V_i > \Sigma_S x_i/\Sigma_S V_i$ and it favors small parties if $\Sigma_L x_i/\Sigma_L V_i < \Sigma_S x_i/\Sigma_S V_i$, where L and S are subsets of $1, 2, \ldots, n$ such that $x_i > x_j$ whenever $i \in L$ and $j \in S$ [3].

At the same time, as mentioned in [16], there are no known such methods that would be used in practice; one and the same APP method in some apportionments can favor, predominantly, large beneficiaries, and in other apportionments, predominantly, small beneficiaries. This is why, as noted in [16], this approach can be used to identify the "total favoring" or "full favoring" of large or small beneficiaries in particular apportionments. It is easy to observe that "full favoring" are particular cases of "favoring" the beneficiaries – large (predominantly) or small (predominantly).

Resuming, Approaches 1-4 can place APP methods in the decreasing order of favoring the small or, on the contrary, the large beneficiaries. Moreover, Approaches 1 and 2 permit to characterize quan-

titatively, to some extent, APP methods: Approach 1 – the relative frequency (probability, on the infinite number of apportionments) of favoring by pairs large or small beneficiaries; Approach 2 – the relative frequency (probability, on the infinite number of apportionments) of favoring the subset of large or the subset of small beneficiaries. In Section 3, there are discussed other informative approaches regarding the degree of favoring the large or the small beneficiaries. First, a systemized vision of favoring the beneficiaries in apportionments is done.

3 Criteria for estimating the degree of favoring

Based on [13, 15], one can distinguish four notions of favoring in apportionments:

a) favoring a decider (voter, etc.) in an apportionment;

b) favoring a beneficiary in an apportionment;

c) favoring large or small beneficiaries in an apportionment;

d) favoring large or small beneficiaries overall by an apportionment method.

Also, as mentioned in [13], each of the specified above four notions can be characterized by:

A) identifying the fact of favoring the deciders or beneficiaries in apportionments;

B) quantitatively estimating the favoring of deciders or beneficiaries in apportionments.

Of course, all quantitative criteria, along with the respective quantitative assessments (aspect B), can be used also to identify the fact of favoring in apportionments (aspect A) [13]. Combining issues A and B with notions (a)-(d), further in this paper the following aspects of favoring in apportionments will be distinguished: Aa, Ab, Ac and Ad and, respectively, Ba, Bb, Bc and Bd.

With refer to proportional apportionments, it is considered that a beneficiary i is favored if a larger number x_i of a-entities is distributed to him than would be due according to the V_i value, that is $x_i > MV_i/V = D_i$, where $M = x_1+x_2+\ldots+x_n$ and $V = V_1+V_2+\ldots+V_n$. In [15], D_i is defined as the free of bias part (rights, influence power, etc.) of beneficiary i in the apportionment; also, $r = M/V$ is defined as the free of bias part (rights, etc.) of a decider in the apportionment, if to consider that V is the total number of deciders. Of course, the lack of favoring is possible only if the equalities $\lfloor MV_i/V \rfloor = MV_i/V, i = \overline{1,n}$ take place; here $\lfloor z \rfloor$ means the integer part of the real number z. In practice, such equalities rarely occur and that is why some beneficiaries are favored and others, respectively, are disfavored.

Definition 1. [15] *In an apportionment, a beneficiary i is favored, if it gets an excess number of a-entities ($\Delta D_i = x_i–D_i > 0$), is disfavored, if it obtains a deficit number of a-entities ($\Delta D_i < 0$), and is neutral (neither favored nor disfavored), if it gets a number of a-entities equal to the expected one ($\Delta D_i = 0$).*

So, the essense of aspect Ab is the following:

1) for the favored beneficiary i, occurs $x_i > a_i$, where $a_i = \lfloor D_i \rfloor$;

2) for the disfavored beneficiary i, occurs $x_i \leq a_i$ at $D_i > a_i$;

3) for the neutral beneficiary i, occurs $x_i = a_i$ at $D_i = a_i$.

Aspect Bb, the degree of favoring the beneficiary i is characterized by the number of a-entities in excess in the apportionment: $\Delta D_i = x_i–D_i$; of course, if $\Delta D_i < 0$, then the beneficiary i is disfavored because it has a deficit of a-entities. Here, it is useful to mention that because of $D_1 + D_2 + \ldots + D_n = M$ and $x_1 + x_2 + \ldots + x_n = M$, if some beneficiaries are favored, the other ones are mandatory disfavored at the same summary extent.

Now, let r_i be the power of influence of a decider that supported the beneficiary i in the apportionment. According to [13], one has $r_i = x_i/Vi, i = \overline{1,n}$.

Definition 2. *(based on [15]) In an apportionment, a decider that supported the beneficiary i is favored if it gets an excess value of influence power ($\Delta r_i = r_i - r > 0$); is disfavored if it obtains a deficit value of influence power ($\Delta r_i < 0$); and is neutral (neither favored nor disfavored) if it gets a value of influence power equal to the expected one ($\Delta r_i = 0$).*

So, the essence of aspect Aa, regarding a decider that supported the beneficiary i, is the following:

1) for the favored decider, occurs $r_i > r$;

2) for the disfavored decider, occurs $r_i < r$;

3) for the neutral decider, occurs $r_i = r$.

Aspect Ba, the degree of favoring of a decider that supported the beneficiary i is characterized by the value of influence power in excess in the apportionment, $\Delta r_i = r_i - r$; of course, if $\Delta r_i < 0$, then the decider is disfavored because it has a deficit of influence power.

Statement 1. *In apportionments, favoring the deciders absolutely correlates with favoring the beneficiaries supported by them.*

Indeed, one has $D_i = MV_i/V$ and $r = M/V$. So, $r = D_i/V_i$. At the same time, $\Delta r_i = r_i - r = x_i/V_i - D_i/V_i = (x_i - D_i)/V_i = \Delta D_i/V_i, i = \overline{1,n}$. ♦

According to Statement 1, if in an apportionment, a beneficiary is favored, then all deciders that supported this beneficiary are favored as well. This is why, above in this section, both these cases (favoring a beneficiary and favoring a decider that supported him) are referred to together as aspect B. However, sometimes it is useful to characterize quantitatively favoring the deciders apart from the characterization of favoring the respective beneficiary.

Statement 2. *The discrepancy of favoring the deciders that supported different beneficiaries (i and $k \neq i$) in apportionments, measured as the difference $\Delta r_i - \Delta r_k$, is equivalent to the one measured as the difference $r_i - r_k$, that is $\Delta r_i - \Delta r_k = r_i - r_k, k \neq i, i = \overline{1,n}$.*

Indeed, one has $\Delta r_i - \Delta r_k = r_i - r - (r_k - r) = r_i - r_k, (i,k) = \overline{1,n}, k \neq i$. ♦

Consequence 1. *Differences $\Delta r_i - \Delta r_k$ and $r_i - r_k$, which characterize the discrepancy of favoring the deciders that supported different beneficiaries (i and $k \neq i$) in apportionments, are interchangeable, but the last one is simpler.*

Thus, in apportionments, the degree of favoring a beneficiary i (aspect Bb) is characterized by the parameter $\Delta D_i (i = \overline{1,n})$, measured in a-entities (aE), and the degree of favoring a decider which supported the beneficiary i (aspect Ba) is characterized by the parameter $\Delta r_i (i = \overline{1,n})$, measured in a-entities/decider (aE/DM). It remains to define criteria for the degree of favoring large or small beneficiaries in an apportionment (aspect Bc), overall by an apportionment method (aspect Bd) and, optionally, of aspects Ac and Ad.

A criterion (F_{a1}) for estimating the degree of favoring the large or small beneficiaries in proportional apportionments (aspect Bc) is proposed in [13]. Further, without diminishing the universality of the approach, it is considered that the n beneficiaries are ordered in the non-ascending order of $V_i, i = \overline{1,n}$ values, that is $V_1 \geq V_2 \geq V_3 \geq \ldots \geq V_n$. Based on these relations, in [12] the L and S subsets of large and, respectively, small beneficiaries were defined as follows: $L = \{1, 2, \ldots, \lfloor n/2 \rfloor\}$ and $S = \{\lceil n/2 \rceil + 1, \lceil n/2 \rceil + 2, \ldots, n\}$, where $x_i \geq x_j$ whenever $i \in L$ and $j \in S$. Here, it should be noted that in proportional apportionments, if $V_i > V_k$, then $x_i \geq x_k$.

Definition 3. [13] *An apportionment favors large beneficiaries if the summary number of a-entities in excess obtained by large beneficiaries (L) is greater than that obtained by small beneficiaries (S), and vice versa; that is, it favors large beneficiaries if $F_{a1} > 0$, it favors the small ones if $F_{a1} < 0$, and it is neutral if $F_{a1} = 0$, where*

$$F_{a1} = \sum_{i \in L} \Delta D_i - \sum_{i \in S} \Delta D_i. \tag{1}$$

Criterion F_{a1} ensures both, the identification of the fact of favoring (aspect Ac) and the estimation of the degree of favoring the large or the

small beneficiaries in an apportionment, measured in a-entities (aspect Bc). Similarly, for APP methods, as a quantitative criterion in [13], the average $\overline{F_{a1}}$ of F_{a1} on the infinity of apportionments is proposed.

Definition 4. [13] *An apportionment method favors large beneficiaries if the average summary number of a-entities in excess obtained by large beneficiaries (L) is greater than that obtained by small beneficiaries (S), and vice versa; that is, it favors large beneficiaries if* $\overline{F_{a1}} > 0$*, it favors the small ones if* $\overline{F_{a1}} < 0$*, and it is neutral if* $\overline{F_{a1}} = 0$*, where* $\overline{F_{a1}}$ *is the average of* F_{a1} *on the infinity of apportionments. So,*

$$\overline{F_{a1}} = \lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} (\sum_{i\in L} \Delta D_{ik} - \sum_{i\in S} \Delta D_{ik}) = \sum_{i\in l} \overline{\Delta D_i} - \sum_{i\in S} \overline{\Delta D_i}, \quad (2)$$

where $\overline{\Delta D_i}$ *is the average of* ΔD_i *on* $K \to \infty$ *apportionments.*

As criterion F_{a1}, the $\overline{F_{a1}}$ one ensures the identification of the fact of favoring (aspect Ad) and the quantitative estimation of the degree of favoring the large or the small beneficiaries by an APP method, measured in a-entities (aspect Bd). Also, from Definition 4 one can conclude that if $\overline{F_{a1}} \neq 0$, then the respective APP method is favoring the beneficiaries (the large ones in case of $\overline{F_{a1}} > 0$ or the small ones in case of $\overline{F_{a1}} < 0$).

Further, the notation $\overline{Y}$ of the average of parameter Y values on the infinity of apportionments will be used.

In addition to criteria $\Delta D_i, \Delta r_i, F_{a1}$ and $\overline{F}_{a1}$ already defined, such quantitative criteria for assessing the favoring of beneficiaries by APP methods may be useful in various situations, especially in research, as:

- The average relative discrepancy between the degree of favoring of an average (conventional) large beneficiary decider and that of an average (conventional) small beneficiary decider $\overline{F_{r1}}$ (%decider-power), where $F_{r1} = 100(r_L - r_S)/r$, $r_L = \sum_{i\in L} x_i / \sum_{i\in L} V_i$, $r_S = \sum_{i\in S} x_i / \sum_{i\in S} V_i$. Here r_L and r_S are the influence power of an average (conventional) large and, respectively, of an average (conventional) small beneficiary decider;

- The average largest absolute discrepancy of the degree of favoring between two beneficiaries $\overline{F_{a0}} = \sum_{i=1}^{n-1}(\overline{\Delta D_i} - \overline{\Delta D_{i+1}}) = \overline{\Delta D_i} - \overline{\Delta D_n}$, a-entities;

- The largest discrepancy of the probability of favoring between two beneficiaries $F_p = \sum_{i=1}^{n-1}(F_{pi} - F_{p,i+1}) = F_{p1} - F_{pn}$. Here F_{pi} is the probability of favoring the beneficiary i in apportionments, that is $F_{pi} = \lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} C_{ik}$, where $C_{ik} = 1$, if $x_i > D_i$, and $C_{ik} = 0$, otherwise;

- The average largest relative discrepancy of the degree of favoring between two deciders which supported different beneficiaries $\overline{F_{r0}}$ (%decider-power - %DP), where $F_{r0} = 100 \sum_{i=1}^{n-1}(r_i - r_{i+1}) = 100(r_1 - r_n)/r$.

Criterion $\overline{F_{a1}}$ allows the absolute evaluation and that of $\overline{F_{r1}}$ – the relative evaluation on r of the degree of favoring the large (L) or the small (S) beneficiaries by the APP method. The next two criteria, $\overline{F_{a0}}$ and F_p, characterize the discrepancy of favoring between the largest ($i = 1$) and the smallest ($i = n$) beneficiaries in the apportionment. Finally, criterion $\overline{F_{r0}}$ characterizes the discrepancy of favoring between a decider which supported the largest ($i = 1$) beneficiary and a decider which supported the smallest ($i = n$) beneficiary; it correlates with $\overline{F_{a0}}$, but is simpler. Anyway, the main criterion, when determining the degree of favoring the beneficiaries by APP methods, is the $\overline{F_{a1}}$ one.

According to Definitions 3 and 4, there is a clear distinction between the degree of favoring the beneficiaries in an apportionment and the degree of favoring the beneficiaries overall by an APP method. For specific apportionments, an APP method may favor particular beneficiaries, both large and small, but overall, on the infinite number of apportionments, be neutral. Namely, the degree of favoring the beneficiaries by an APP method overall, on the infinite number of apportionments, will be investigated thereafter in this paper.

4 Overview of computer simulation of favoring

In total, 6 APP methods are investigated, namely the Hamilton (Hare) - H, d'Hondt (Jefferson) - d'H, Huntington-Hill (HH), Adapted Sainte-Laguë (ASL), Variable linear divisor (VLD) and Quota dependent linear divisor (QDLD) ones. All these methods are described, for example, in [17].

In order to determine the values of quantitative criteria $\overline{F_{a0}}$, $\overline{F_{r0}}$, $\overline{F_{a1}}$, $\overline{F_{r1}}$ and $\overline{F_p}$, computer simulation using SIMAP application was performed. Initial data used in calculations are: M = 6, 11, 21, 51, 101, 201, 501; n = 2, 3, 4, 5, 7, 10, 15, 20, 30, 50; $n \leq M$–1; $V = 10^8$; uniform distribution of the values $V_i, i = \overline{1,n}$; sample size 10^6. So, we have 58 variants of values for the pair $\{M, n\}$: 4 + 6 + 8 + 10 = 58. The use of small values of M is useful, for example, when determining the M members of a parliamentary committee basing on the number of deputies (V_i) of each of the n parties in the Parliament. Sometimes, from the specified above 58 variants, only 50 are used – variants for which $n \leq M/2$. This is because cases in which $M/2 < n < M$ are rarely encountered in practice, but the apportionment disproportion when applying the Huntington-Hill and adapted Sainte-Laguë methods in such cases increases considerably. Some of the obtained results are described below.

5 Preferenced APP methods by non-favoring the beneficiaries

Some results of calculations for the average value (on 50 variants of the pair of sizes for M and n values) of criteria $\overline{F_{a0}}$, $\overline{F_{a1}}$, $\overline{F_{r1}}$ and $\overline{F_p}$ at $n \leq M/2$ are systemized in Table 1. In more detailes, for the pair $\{M, n\}$ at $n \leq M/2$ one has 50 variants of values described in Section 4. For each such pair of values, 1 mil variants of values for $\{V_i, i = \overline{1,n}\}$ sizes were generated randomly, at uniform distribution, thus being obtained 1 mil variants of the APP problem initial data; for each such variant, calculations were done, and after that, there were obtained the average values of the explored parameters. Finally, there were also calculated the average values of the explored criteria on 50

variants of pair $\{M, n\}$ values. So, for each of the 6 explored methods, calculi were done on $50 \times 1000000 = 50$ mil apportionments.

Table 1. Results for $\overline{F_{a0}}, \overline{F_{a1}}$, $\overline{F_p}$ and $\overline{F_{r1}}$ at $n \leq M/2$

Criterion	APP method and the average value of criterion on 50 variants of the pair $\{M, n\}$ sizes					
$\overline{F_{a1}}$, a-entities	VLD $\succ$	H $\succ$	ASL$\succ$	HH $\succ$	QDLD $\succ$	d'H $\succ$
	0.02014	0.04040	-0.71040	-0.92720	-2.18101	2.50428
$\overline{F_{r1}}$, %DP	VLD $\succ$	H $\succ$	ASL$\succ$	HH $\succ$	QDLD $\succ$	d'H $\succ$
	0.23809	0.34620	-4.08271	-4.99704	-5.42261	8.99951
$\overline{F_{a0}}$, a-entities	VLD $\succ$	H $\succ$	ASL$\succ$	HH $\succ$	QDLD $\succ$	d'H $\succ$
	0.03590	0.03882	-0.26795	-0.31000	-0.42923	0.66386
$100F_p$, %	VLD $\succ$	H $\succ$	ASL$\succ$	HH $\succ$	QDLD $\succ$	d'H $\succ$
	9,840	10,125	-20,290	-24,420	-36,681	68,644

In Table 1, the positive values of used criteria correspond to cases of favoring large beneficiaries, and the negative ones – to cases of favoring small beneficiaries. The values of criteria for the VLD, H and d'H methods are positive, and those for the ASL, HH and QDLD (at $n > 3$) methods are negative. Of course, there is no doubt about the Hamilton method neutrality with refer to favoring the beneficiaries overall, on the infinity of apportionments (see, for example, [17]). Also, the average value of criterion $\overline{F_{a1}}$ for Hamilton method is of 0.04040 a-entities, that is 17.6 times smaller than that for Adapted Sainte-Laguë method. So, taking into account the limited precision of computer simulation, according to Table 1, one can conclude that:

1) VLD and H (as is well-known) methods are neutral in favoring the beneficiaries;

2) ASL, HH (as is well-known) and QDLD (at $n > 3$) methods favor small beneficiaries;

3) d'H method favors large beneficiaries (as is well-known).

It should be mentioned that in Table 1 the relation A $\succ$ B of method A preference to method B is done by the absolute value of used criteria. Also, despite the limited accuracy, the results of calculations are

obtained for the same initial data sets and can therefore be used in the comparative analysis for all methods.

From Table 1, one can see that preferences of APP methods by criteria $\overline{F_{a1}}, \overline{F_{r1}}$ and F_p coincide. So, all criteria $\overline{F_{r1}}, \overline{F_{a0}}$ and F_p can be used to identify the fact of favoring by APP methods, but the last two are simpler than the $\overline{F_{a1}}$ and $\overline{F_{r1}}$ ones. Also, one can say that the preferences of examined 6 APP methods in non-favoring of beneficiaries are the following: VLD $\succ$ H $\succ$ ASL $\succ$ HH $\succ$ QDLD $\succ$ d'H.

Obtained average values of the explored criteria on the 50 variants of the pair $\{M, n\}$ values allow, to some extent, the overall determination of the APP methods preferences regarding the favoring of beneficiaries. At the same time, additional information can be obtained using similar calculations for each of the 58 variants of the pair $\{M, n\}$ values.

Overall, the degree of favoring of beneficiaries by APP methods is determined by criterion $\overline{F_{a1}}$ or the $\overline{F_{r1}}$ one. The more specific criteria $\overline{F_{a0}}$, $\overline{F_{r0}}$, and F_p can also be used for this purpose. Selective results of calculations according to criteria $\overline{F_{a1}}$, $\overline{F_{r1}}$, $\overline{F_{a0}}$, and $\overline{F_{r0}}$ for the d'Hondt, Adapted Sainte-Laguë, Huntington-Hill, and QDLD methods are described in Section 6.

6 Degree of favoring by some APP methods

The graphs of criteria $\overline{F_{a0}}, \overline{F_{a1}}$, and $\overline{F_{r1}}$ dependence on M and n for **d'Hondt method** are shown in Figures 1-2a. Characterizing the largest absolute discrepancy of the degree of favoring between two beneficiaries, the criterion $\overline{F_{a0}}$ (Figure 1) most easily identifies the fact of favoring the large or the small beneficiaries in case of separate pairs of values of sizes M and n.

From Figure 1a, it can be seen that out of the 58 variants of the pair $\{M, n\}$ values, the largest average absolute discrepancy $\overline{F_{a0}}$(d'H) between the largest ($i = 1$) and the smallest ($i = n$) beneficiary is obtained for the pair $\{M = 501, n = 20\}$, this being equal to approx. 0.9 a-entities. For $\{6 \leq M \leq 501,\ M \geq 2n\}$, this discrepancy is in the range of $0.32 \div 0.39$ aE at $n = 2$, of $0.51 \div 0.56$ aE at $n = 3$, of $0.62 \div 0.65$ aE at $n = 4$, of $0.71 \div 0.84$ aE at $n = 10$, of $0.69 \div 0.89$ aE at $n = 20$, and of $0.55 \div 0.79$ aE at $n = 50$, being considerable.

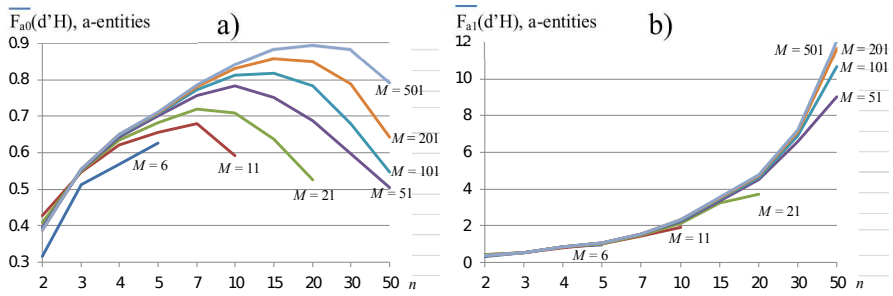


Figure 1. Criteria $\overline{F_{a0}}$ and $\overline{F_{a1}}$ dependences to M and n for d'H method.

Figure 1b shows that the value $\overline{F_{a1}}$(d'H) is increasing to n and slightly increasing to M, especially at $M \geq 2n$. For $\{6 \leq M \leq 501, 2 \leq n \leq 50,\ n < M\}$, the $\overline{F_{a1}}$(d'H) value is between $0.32 \div 0.41$ aE (at $n = 2$), and $9.0 \div 12.1$ aE (at $n = 50$), being considerable at relatively high values of n. Under the same conditions, but $n \leq M/2$, the $\overline{F_{a1}}$(d'H) value at $n = 50$ is in the range of $10.7 \div 12.1$ aE.

Criterion $\overline{F_{r1}}$ compares the average influence of a decider belonging to the group of large beneficiaries ($i = 1, 2, \ldots, \lfloor n/2 \rfloor$) with that of a decider belonging to the group of small beneficiaries ($i = \lfloor n/2 \rfloor + 1, \lfloor n/2 \rfloor + 2, \ldots, n$). The discrepancy $\overline{F_{r1}}$(d'H) is decreasing with respect to M and is increasing with respect to n (Figure 2a). At high values of n and low values of M, this discrepancy is considerable. Thus, for initial data stated in Section 4, they belong to the range of $0.43 \div 35.32$ %decider-power at $n = 4$, of $0.73 \div 53.00$ %DP at $n = 5$, of $1.20 \div 44.77$ %DP at $n = 10$, and of $6.36 \div 46.67$ %DP at $n = 50$. If $n \leq M/2$, the discrepancy $\overline{F_{r1}}$(d'H) is within the range of $0.43 \div 18.50$ %DP at $n = 4$, of $0.73 \div 30.88$ %DP at $n = 5$, of $1.20 \div 26.28$ %DP at $n = 10$, and of $6.36 \div 27.90$ %DP at $n = 50$.

The graphs of criteria $\overline{F_{a0}}, \overline{F_{a1}}$, and $\overline{F_{r1}}$ values dependence on M and n, using the Huntington-Hill method, are shown in Figures 2b-3.

Figure 2b shows that discrepancy $|\overline{F_{r1}}(\text{HH})|$ is decreasing on M and is increasing on n. For $\{6 \leq M \leq 501,\ 2 \leq n \leq 50,\ n \leq M/2\}$, the $|\overline{F_{r1}}(\text{HH})|$ values belong to the range of $0.0014 \div 10.63$ %DP at $n = 2$, of $0.0092 \div 33.36$ %DP at $n = 3$, of $0.010 \div 12.01$ %DP at $n = 4$, of

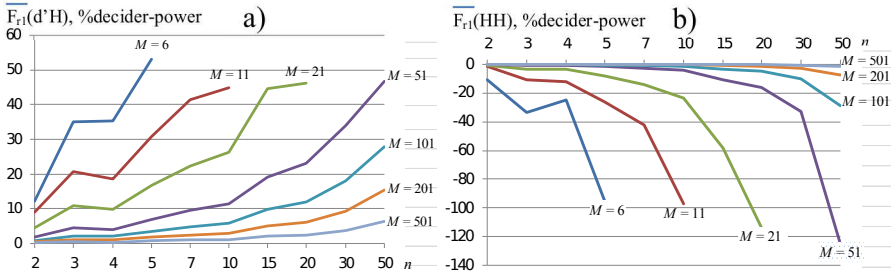


Figure 2. Criterion $\overline{F_{r1}}$ dependence to M and n for d'H and HH methods.

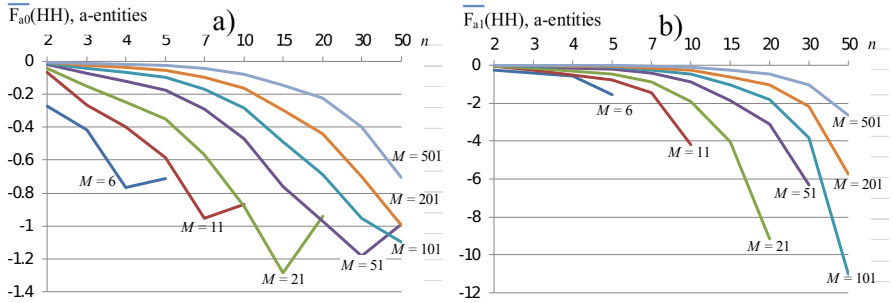


Figure 3. Criteria $\overline{F_{a0}}$ and $\overline{F_{a1}}$ dependences to $\{M, n\}$ for HH method.

$0.065 \div 23.33$ %DP at $n = 10$, and of $1.40 \div 28.80$ %DP at $n = 50$.

According to Figure 3a, out of the 58 variants of the pair $\{M,\ n\}$ values, the largest average absolute discrepancy between the largest ($i = 1$) and the smallest ($i = n$) beneficiary, $\overline{F_{a0}}$(HH), is obtained in case of $\{M = 21,\ n = 15\}$ and is equal to approx. -1.28 a-entities. The discrepancy $|\overline{F_{a0}}(\text{HH})|$ is decreasing on M and is increasing on n. At $\{6 \leq M \leq 501,\ n \leq M/2\}$, the $|\overline{F_{a0}}(\text{HH})|$ values belong to the range of $0.0041 \div 0.27$ a-entities at $n = 2$, of $0.011 \div 0.42$ aE at $n = 3$, of $0.017 \div 0.40$ aE at $n = 4$, of $0.078 \div 0.88$ aE at $n = 10$, and of $0.71 \div 1.10$ aE at $n = 50$.

As in case of $\overline{F_{a1}}$(d'H), the $|\overline{F_{a1}}(\text{HH})|$ value is increasing on n (Figure 3b). But unlike $\overline{F_{a1}}$(d'H), the $|\overline{F_{a1}}(\text{HH})|$ value is pronounced decreasing on M. For $\{6 \leq M \leq 501, 2 \leq n \leq 50,\ n < M\}$, the $|\overline{F_{a1}}(\text{HH})|$ values belong to the range of $0.0041 \div 0.27$ a-entities at $n = 2$, of $0.0011 \div 0.41$ aE at $n = 3$, of $0.020 \div 0.60$ aE at $n = 4$, of $0.13 \div 4.17$ aE at $n = 10$, and of $2.65 \div 24.18$ aE at $n = 50$, being considerably smaller compared to those of $\overline{F_{a1}}$(d'H). At high values of M, the $|\overline{F_{a1}}(\text{HH})|$ values are less significant. For example, for $M = 501$, the $|\overline{F_{a1}}(\text{HH})|$ value is equal to 0.0041 aE at $n = 2$ and to 2.65 aE at $n = 50$.

Graphs of criteria $\overline{F_{a0}}, \overline{F_{a1}}$ and $\overline{F_{r1}}$ dependences on M and n, when using the **Adapted Sainte-Laguë method**, are largely similar to those for the Huntington-Hill method. Some quantitative differences can be found in Figures 5a-6b and Tables 2-4.

Graphs of criteria $\overline{F_{a0}}$ and $\overline{F_{a1}}$ dependences on M and n, when using the **QDLD method**, are shown în Figure 4. In these graphs, it is taken into account that at $n = 2$ and $n = 3$ the QDLD method coincides with the Sainte-Laguë one; that is, it is neutral regarding favoring the beneficiaries. That is why $4 \leq n \leq 50$.

From Figure 4a, it can be seen that out of the 58 values of the pair of sizes M and n, the largest average absolute discrepancy $\overline{F_{a0}}$(QDLD) between the largest ($i = 1$) and the smallest ($i = n$) beneficiary is obtained in case of $\{M = 201,\ n = 50\}$, this being equal to approx. -1.15 a-entities. Discrepancy $|\overline{F_{a0}}(\text{QDLD})|$ almost does not depend on M and is decreasing with respect to n except for cases when $n = M-1$, in which it also little depends on n. At $\{n \leq M/2,\ 6 \leq M \leq 501\}$, this discrepancy is in the range of $0.16 \div 0.21$ a-entities at $n = 4$, of

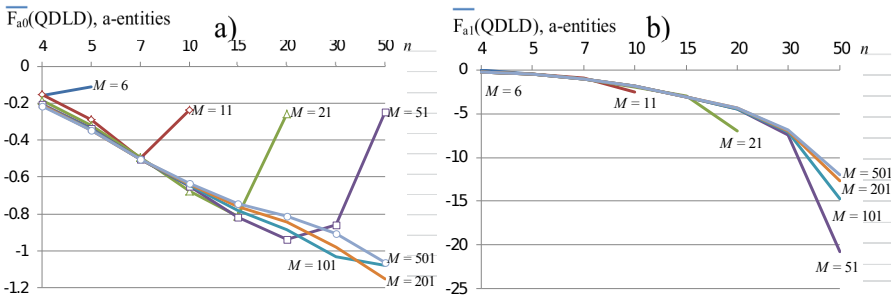


Figure 4. Criteria $\overline{F_{a0}}$ and $\overline{F_{a1}}$ dependences to $\{M, n\}$ for QDLD method.

$0.11 \div 0.35$ aE at $n = 5$, of $0.63 \div 0.67$ aE at $n = 10$, and of $0.55 \div 0.79$ aE at $n = 50$.

Figure 4b shows that the $|\overline{F_{a1}}(\text{QDLD})|$ value is ascending to n, but is slightly decreasing to M; at the same time, at $n \leq M/2$ the $|\overline{F_{a1}}(\text{QDLD})|$ value little depends on M. For $\{11 \leq M \leq 501,\ 4 \leq n \leq 50,\ n \leq M/2\}$, the $|\overline{F_{a1}}(\text{QDLD})|$ value belongs to the range of $0.24 \div 0.29$ a-entities at $n = 4$, of $0.45 \div 0.52$ aE at $n = 5$, of $1.80 \div 1.96$ aE at $n = 10$, and of $12.04 \div 14.69$ aE at $n = 50$, being considerable, especially at high values of n.

7 Comparative analyses of favoring the beneficiaries by APP methods

Let's first examine the Huntington-Hill and Adapted Sainte-Laguë methods, which guarantee the allocation of at least one a-entity to each beneficiary. For quantitative comparative estimates, Figures 5a and 5b show the graphs of the difference $\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL) and those of the ratio $\overline{F_{a1}}$(HH)/$\overline{F_{a1}}$(ASL) dependences on M and n.

From Figure 5a, it can be seen that the favoring of small beneficiaries by Huntington-Hill method is stronger than that obtained by the Adapted Sainte-Laguë one; only at values of n close to those of M it can be $\overline{F_{a1}}(\text{HH}) = \overline{F_{a1}}(\text{ASL})$. The difference $|\overline{F_{a1}}(\text{HH})\text{-}\overline{F_{a1}}(\text{ASL})|$ is

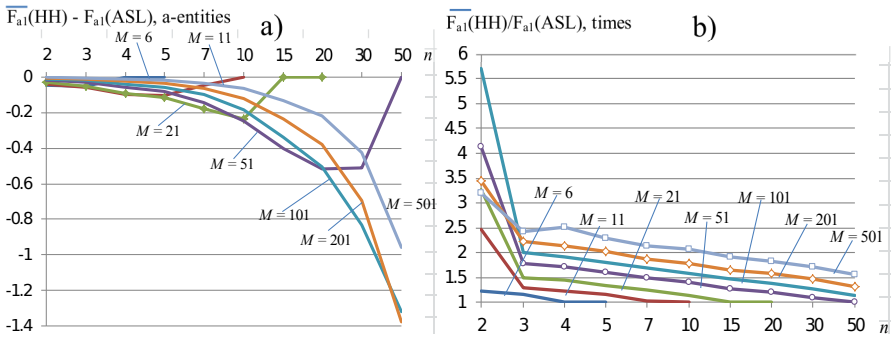


Figure 5. Difference $\overline{F_{a1}}$(HH)$-\overline{F_{a1}}$(ASL) and ratio $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL) dependences to $\{M, n\}$.

also small at low values of n. Thus, the difference $|\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$|$ increases, and then it decreases, both with respect to n and with respect to M. The exception is only the case of $n = 2$, in which, according to calculations, this difference only decreases on M.

For $\{6 \le M \le 501, 2 \le n \le 50,\ n < M\}$, the value $|\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$|$ is between $0.029 \div 0.048$ a-entities at $n = 2$, of $0 \div 1.37$ aE at $n = 50$ and of $0.96 \div 1.37$ aE at $\{n = 50,\ M = 101 \div 501\}$. The highest value of the difference $|\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$|$, equal to 1.37 aE, is at $\{M = 201,\ n = 50\}$.

If, at low values of n, the difference $|\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$|$ values are also small, then those of ratio $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL), on the contrary, are relatively high (Figure 5b), reaching 5.70 times at $\{M = 101,\ n = 2\}$. The ratio $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL) value is decreasing on n, and at $n > 2$ it is increasing on M. For example, if $M = 501$, then $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL) value is approx.2.42 times at $n = 3$ and of approx.2.52 times at $n = 4$; also, $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL) ≈ 1.57 times at $n = 50$. For $\{6 \le M \le 501, 2 \le n \le 50,\ n < M\}$, the $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL) value is between $1 \div 1.57$ times at $n = 50$, of $1.14 \div 1.57$ times at $\{n = 50,\ M = 101 \div 501\}$, and of $1.21 \div 5.70$ times at $n = 2$. The highest value of ratio $\overline{F_{a1}}$(HH)$/\overline{F_{a1}}$(ASL), equal to 5.70 times, is at $\{M = 101,\ n = 2\}$. Undoubtedly, **Huntington-Hill method favors the beneficiaries stronger than the Adapted Sainte-Laguë one does**.

A clear vision of the Adapted Sainte-Laguë method superiority on non-favoring over the Huntington-Hill one is also done by the comparison based on criterion $\overline{F_{r1}}$. Figures 6a and 6b show the graphs of the difference $\overline{F_{r1}}$(HH)-$\overline{F_{r1}}$(ASL) and, respectively, of the ratio $\overline{F_{r1}}$(HH)/$\overline{F_{r1}}$(ASL) dependences on M and n.

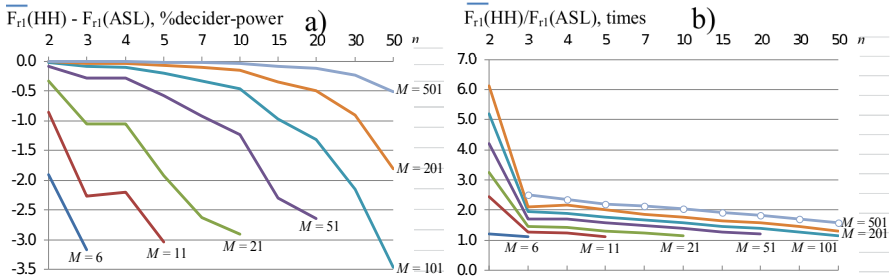


Figure 6. Difference $\overline{F_{r1}}$(HH)$-\overline{F_{r1}}$(ASL) and ratio $\overline{F_{r1}}$(HH)/$\overline{F_{r1}}$(ASL) dependences to $\{M, n\}$.

For initial data stated in Section 4, the inequality $|\overline{F_{r1}}(\text{HH})| > |\overline{F_{r1}}(\text{ASL})|$ occurs, except the cases of $n = M - 1$ for which $\overline{F_{r1}}$(HH) = $\overline{F_{r1}}$(ASL). That is, the Huntington-Hill method favors beneficiaries stronger than the adapted Sainte-Laguë one does, the difference in question reaching 3.47 %decider-power at $\{M = 101, n = 50\}$. At $\{6 \le M \le 501,\ n \le M/2\}$, the difference $|\overline{F_{r1}}(\text{HH})|$-$|\overline{F_{r1}}(\text{ASL})|$ value is decreasing on M and is increasing on n (Figure 6a).

If between the case of $n = 2$ and the other cases of graphs in Figure 5a there is some discrepancy regarding the value of ratio $\overline{F_{a1}}$(HH)/$\overline{F_{a1}}$(ASL), then in case of ratio $\overline{F_{r1}}$(HH)/$\overline{F_{r1}}$(ASL) such a discrepancy is missing (Figure 6b): the increase of M always results with the increase of the ratio in question. At the same time, the ratio $\overline{F_{r1}}$(HH)/$\overline{F_{r1}}$(ASL) dependence on n is decreasing.

Although the d'Hondt method does not guarantee the allocation of at least one a-entity to each beneficiary, such as Huntington-Hill and Adapted Sainte-Laguë do, for comparison in Figure 7a the ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})|$ dependence to M and n is given, without the cases of $M = 501$ and also those of $n = 2$.

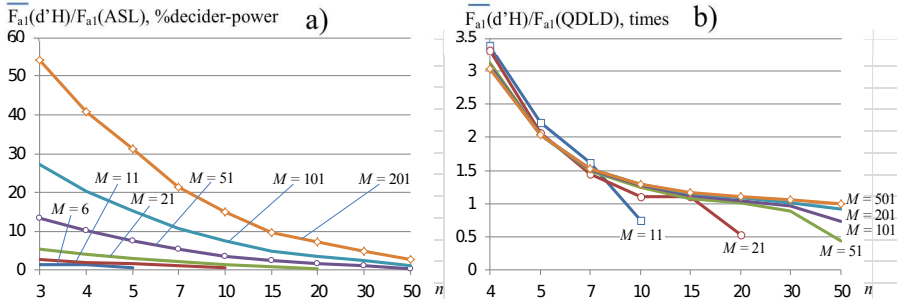


Figure 7. Ratios $\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(ASL) and $\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(QDLD) dependences to $\{M, n\}$.

It can be seen that the ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})|$ value is decreasing on n, but is increasing on M. For $\{6 \le M \le 501, 2 \le n \le 50,\ n < M\}$, the $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})|$ values belong to the range of $0.37 \div 7.13$ times at $n = 50$, of $1.10 \div 7.13$ times at $\{n = 50,\ M = 101 \div 501\}$, of $0.63 \div 76.7$ times at $n = 5$, and of $1.42 \div 301$ times at $n = 2$. For very many cases, the value of this ratio exceeds 10 times. Values lower than 1 are obtained only for very specific cases, usually not encountered in practice: $\{M = 6, n = 5\}, \{M = 11, n = 10\}, \{M = 21, n = 15\}, \{M = 21, n = 20\}$, and $\{M = 51, n = 50\}$. It can be considered that **usually d'Hondt method favors beneficiaries much stronger than the Adapted Sainte-Laguë one does**.

It should be noted that QDLD method can be used under same conditions as the d'Hondt method. For comparison, in Figure 7b is given the ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})|$ dependence on M and n, without the cases of $n = 2$ and $n = 3$, in which the QDLD method does not favor beneficiaries, and also without the case of $M = 6$. One can observe the ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})|$ decreasing dependence on n and its weak dependence on M at relatively high values of M and n. In more detail, according to the results of calculations, compared to M, the ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})|$ value is decreasing at $n = 4$ and $n = 5$; is increasing at $n = 10$, $n = 20$, $n = 30$; and $n = 50$; and is first decreasing (at $\{n = 7, 11 \le M \le 21\}$ and $\{n = 15, 21 \le M \le 51\}$) and

then is increasing.

In case of $M = 6$, the value of examined ratio is of 91.2 times at $n = 4$ and of 2.25 times at $n = 5$. For $\{11 \leq M \leq 501, 4 \leq n \leq 50, n < M\}$, the $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})|$ values belong to the range of $0.43 \div 1.00$ times at $n = 50$, of $0.73 \div 1.00$ times at $\{n = 50, 101 \leq M \leq 501\}$, of $1.45 \div 1.62$ times at $n = 7$, and of $3.04 \div 3.38$ times at $n = 4$. Values less than 1 are obtained only for very specific cases, usually not encountered in practice: $\{M = 11, n = 10\}$, $\{M = 21, n = 20\}$, $\{M = 51, n = 30 \div 50\}$, $\{M = 101, n = 30 \div 50\}$, and $\{M = 201, n = 50\}$. Therefore, it can be considered that **usually d'Hondt method favors beneficiaries stronger than the QDLD one does**.

The character of dependences $\overline{F_{a1}}$, $\overline{F_{r0}}$, and $\overline{F_{r1}}$ of favoring the beneficiaries by the four APP methods to M and n at $n \leq M/2$ is shown in Table 2.

Table 2. Character of some dependences to M and n at $n \leq M/2$

Dependences	Apportionment methods			
	HH	ASL	d'H	QDLD
Dependence $\overline{F_{r0}}$ and $\overline{F_{r1}}$ on M	strongly decreasing	strongly decreasing	strongly decreasing	strongly decreasing
Dependence $\overline{F_{a1}}$ on M	strongly decreasing	strongly decreasing	slightly increasing	slightly decreasing
Dependence $\overline{F_{r0}}$, $\overline{F_{r1}}$ and $\overline{F_{a1}}$ on n	increasing	increasing	increasing	increasing

From Table 2, for the four examined methods, it can be seen that:

- the nature of criteria $|\overline{F_{r0}}|$ and $|\overline{F_{r1}}|$ dependences on M and n and also of the $|\overline{F_{a1}}|$ one on n is the same in all methods. Regarding the nature of the $|\overline{F_{a1}}|$ dependence on M, it coincides for the Huntington-Hill and Adapted Sainte-Laguë methods, being strongly decreasing; it slightly differs for the QDLD method, this being only slightly decreasing, and is completely different for the d'Hondt method, this being slightly increasing;

- the limits of the value ranges of $|\overline{F_{r0}}|$ and those of $|\overline{F_{a1}}|$ and $|\overline{F_{r1}}|$ for the Adapted Sainte-Laguë method are smaller than those

Table 3. Some features of APP methods regarding favoring at $n \leq M/2$

Criteria	n	Apportionment methods			
		HH	ASL	d'H	QDLD
$\lvert\overline{F_{r0}}\rvert$, %DP	2	0.0014÷10.63	0.0000 ÷ 8.72	0.18 ÷ 12.34	0
	3	0.0092÷33.36	0.0037÷30.20	0.46 ÷ 35.10	0
	4	0.027 ÷ 28.56	0.012 ÷ 25.35	0.84 ÷ 35.49	0.28 ÷ 9.02
	7	0.21 ÷ 60.21	0.12 ÷ 57.15	2.57 ÷ 52.04	1.71 ÷ 41.02
	10	0.73 ÷ 181.58	0.47 ÷ 180.11	5.14 ÷ 86.25	4.06 ÷ 108.93
$\lvert\overline{F_{a1}}\rvert$, aE	2	0.0041 ÷ 0.27	0.0013 ÷ 0.22	0.32 ÷ 0.41	0
	3	0.011 ÷ 0.42	0.0044 ÷ 0.36	0.51 ÷ 0.56	0
	4	0.020 ÷ 0.54	0.0078 ÷ 0.44	0.83 ÷ 0.87	0.0094 ÷ 0.29
	10	0.13 ÷ 1.91	0.062 ÷ 1.67	2.15 ÷ 2.34	1.80 ÷ 1.96
	50	2.65 ÷ 11.00	1.69 ÷ 9.68	10.65 ÷ 12.06	12.04 ÷ 14.69
$\lvert\overline{F_{r1}}\rvert$, %DP	2	0.0014÷10.63	0.0000 ÷ 8.72	0.18 ÷ 12.34	0
	3	0.0092÷33.36	0.0037÷30.20	0.46 ÷ 35.10	0
	4	0.010 ÷ 12.01	0.0043 ÷ 9.81	0.43 ÷ 18.50	0.14 ÷ 5.46
	10	0.065 ÷ 23.33	0.032 ÷ 20.41	1.20 ÷ 26.28	0.92 ÷ 23.91
	50	1.40 ÷ 28.80	0.89 ÷ 25.33	6.36 ÷ 27.90	6.36 ÷ 38.46

for the Huntington-Hill method. In turn, the latter are usually smaller than those for the d'Hondt method; some exceptions occur for relatively high values of n, when the requirement to allocate at least one a-entity to each beneficiary strongly influences apportionments;

- the limits of the value ranges of $\lvert\overline{F_{r0}}\rvert$ and those of $\lvert\overline{F_{a1}}\rvert$ and $\lvert\overline{F_{r1}}\rvert$ for the QDLD method in most cases are smaller than those for d'Hondt method.

The absolute degree ($\overline{F_{a1}}$) and those relative to r ($\overline{F_{r0}}$ and $\overline{F_{r1}}$) of favoring by the four APP methods are systematized in Table 3. Also, the character of dependencies $\lvert\overline{F_{a1}}(\text{HH})/\overline{F_{a1}}(\text{ASL})\rvert$, $\lvert\overline{F_{a1}}(\text{HH}) - \overline{F_{a1}}(\text{ASL})\rvert$, $\lvert\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})\rvert$, and $\lvert\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})\rvert$ of favoring the beneficiaries by the four APP methods to M and n at $n \leq M/2$ is systematized in Table 4. The absolute comparative degree of favoring the beneficiaries by examined APP methods is systematized in Table 5. If at $n \leq M$–1 the value of the difference $\lvert\overline{F_{a1}}(\text{HH}) - \overline{F_{a1}}(\text{ASL})\rvert$ is

Table 4. Character of some comparative dependencies at $n \leq M/2$

Dependencies	Comparison criteria			
	$\lvert\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$\rvert$, a-entities	$\lvert\overline{F_{a1}}$(HH)/$\overline{F_{a1}}$(ASL)$\rvert$, times	$\lvert\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(ASL)$\rvert$, times	$\lvert\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(QDLD)$\rvert$, times
Dependence on M	increasing at n-10, then decreasing	increasing at $n = 2$, then decreasing	decreasing	decreasiong at n = 4-5, slightly increasing at $n > 7$
Dependence on n	increasing	increasing	increasing	increasing

first increasing and then decreasing both on M and n (see Figure 5a), then at $n \leq M/2$ it is only increasing to n (see Table 3).

Regarding the dependence on M at $n \leq M/2$ according to the results of calculations, the difference $|\overline{F_{a1}}(\text{HH})-\overline{F_{a1}}(\text{ASL})|$ is first increasing only in two cases, namely at $\{n = 3,\ 6 \leq M \leq 11\}$ and at $\{n = 10,\ 21 \leq M \leq 51\}$, in the other cases being only decreasing.

If the value of $\overline{F_{a1}}(\text{HH})/\overline{F_{a1}}(\text{ASL})$ ratio is significantly greater than 1, obtaining values in the range of $1.14 \div 5.70$ times, then the $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})|$ one can be, depending on the case, considerably higher than 1, obtaining values from 1.10 times to 301 times. That is, in terms of favoring the beneficiaries, **Huntington-Hill method yields significantly, and the d'Hondt method - considerably to the Adapted Sainte-Laguë method**. Also, **d'Hondt method yields absolutely to the QDLD one, at $n = 2$ and $n = 3$, and - significantly, in the other cases of practical interest** (only in cases of $\{M = 101,\ 30 \leq n \leq 50\}$ and of $\{M = 101,\ n = 50\}$ occurs $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})| < 1$). Some details on the largest and the lowest value of the difference $\overline{F_{a1}}(\text{HH})-\overline{F_{a1}}(\text{ASL})$ are systematized in Table 6. According to Table 6, the lowest values of $|\overline{F_{a1}}(\text{HH})-\overline{F_{a1}}(\text{ASL})|$ are obtained at $M = 501$, regardless of the value of n. At the same time, the value of M, at which the highest values of the difference $|\overline{F_{a1}}(\text{HH})-\overline{F_{a1}}(\text{ASL})|$ are obtained, increases on n, the difference in question reaching 1.37 times at $\{n = 50, M = 201\}$ and $M/n \approx 3 \div 4$.

Table 5. The value range of comparison criteria at $n \leq M/2$

n	Comparison criteria			
	$\lvert\overline{F_{a1}}$(HH)-$\overline{F_{a1}}$(ASL)$\rvert$, a-entities	$\lvert\overline{F_{a1}}$(HH)/$\overline{F_{a1}}$(ASL)$\rvert$, times	$\lvert\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(ASL)$\rvert$, times	$\lvert\overline{F_{a1}}$(d'H)/$\overline{F_{a1}}$(QDLD)$\rvert$, times
2	$0.0029 \div 0.048$	$1.21 \div 5.70$	$1.42 \div 301$	∞
3	$0.0063 \div 0.060$	$1.50 \div 2.42$	$1.42 \div 126$	∞
4	$0.012 \div 0.097$	$1.22 \div 2.52$	$1.88 \div 111$	$3.04 \div 3.38$
5	$0.018 \div 0.12$	$1.15 \div 2.29$	$1.51 \div 76.7$	$2.03 \div 2.23$
7	$0.033 \div 0.18$	$1.24 \div 2.14$	$2.05 \div 53.5$	$1.45 \div 1.52$
10	$0.065 \div 0.25$	$1.14 \div 2.06$	$1.29 \div 38.0$	$1.10 \div 1.30$
15	$0.13 \div 0.40$	$1.28 \div 1.91$	$2.32 \div 24.5$	$1.07 \div 1.17$
20	$0.22 \div 0.52$	$1.20 \div 1.82$	$1.74 \div 18.1$	$1.01 \div 1.11$
30	$0.43 \div 0.83$	$1.28 \div 1.71$	$2.31 \div 12.0$	$0.97 \div 1.05$
50	$0.96 \div 1.37$	$1.14 \div 1.57$	$1.10 \div 7.13$	$0.73 \div 1.001$

Table 6. The $|\overline{F_{a1}}(\text{HH}) - \overline{F_{a1}}(\text{ASL})|$ largest and the lowest values at $n \leq M/2$, a-entities

	Number of beneficiaries (n)							
	2	3	4	5	7	10	20	50
M	6	11	11	21	21	51	51	201
$max\lvert\overline{F_{a1}}$(HH)-$\overline{F_{a1}}(ASL)\rvert$	0.048	0.060	0.097	0.12	0.18	0.25	0.83	1.37
M	501	501	501	501	501	501	501	501
$min\lvert\overline{F_{a1}}$(HH)-$\overline{F_{a1}}(ASL)\rvert$	0.003	0.006	0.012	0.012	0.033	0.065	0.22	0.96

8 Conclusions

Based on four notions and two issues (the fact and the quantitative estimate), there are distinguished eight aspects of favoring in apportionments. Mainly, the four quantitative aspects were explored. In this aim, five criteria were defined: the degree of favoring of large or of small beneficiaries by apportionment methods ($\overline{F_{a1}}$), the average largest absolute discrepancy of the degree of favoring between two beneficiaries ($\overline{F_{a0}}$), the average relative discrepancy between the degree of favoring of an average large beneficiary decision-maker and that of an average small beneficiary decision-maker ($\overline{F_{r1}}$), the average largest relative discrepancy of the degree of favoring between two deciders which supported different beneficiaries ($\overline{F_{r0}}$), and the largest discrepancy of the probability of favoring between two beneficiaries (F_p). The degree of favoring is measured in apportioned entities, percentage of decider-power or percentage of apportioned entities. A total of 6 APP methods are being researched, namely, Hamilton (Hare), d'Hondt (Jefferson), Huntington-Hill, Adapted Sainte-Laguë, Variable linear divisor and Quota dependent linear divisor. Hamilton method, neutral in terms of favoring, is investigated only for the purpose of comparative analysis of characteristics of other APP methods considered almost neutral on favoring.

In order to determine the values of quantitative criteria, computer simulation by SIMAP application was used for 58 variants of values for the pair $\{M, n\}$, uniform distribution of values $V_i, i = \overline{1, n}$ and sample size of 10^6. Done calculations not only confirmed some known preferences with refer to non-favoring the beneficiaries, but also permitted to estimate quantitatively the degree of favoring the beneficiaries by the 6 APP methods. For example, it was identified that:

- preferences among 6 APP methods, with refer to non-favoring of beneficiaries by criteria $\overline{F_{a1}}$, $\overline{F_{a0}}$, $\overline{F_{r1}}$ and F_p, coincide;
- the degree of favoring of beneficiaries depends both, on APP method used and on the value of initial data, and can be considerable. For example, the $\overline{F_{a1}}$(d'H) value is increasing to n and slightly increasing to M, and $9.0 \leq \overline{F_{a1}}(\text{d'H}) \leq 12.1$ (a-entities) at $\{n = 50,\ 51 \leq M \leq 501\}$;

- Huntington-Hill method favors small beneficiaries stronger than the Adapted Sainte-Laguë one does. The highest value of the difference $|\overline{F_{a1}}(\text{HH}) - \overline{F_{a1}}(\text{ASL})|$, equal to 1.37 a-entities, is at $M = 201$ and $n = 50$. The highest value of ratio $\overline{F_{a1}}(\text{HH})/\overline{F_{a1}}(\text{ASL})$, equal to 5.70 times, is at $\{M = 101,\ n = 2\}$;
- usually d'Hondt method favors beneficiaries much stronger than the Adapted Sainte-Laguë one does. For very many cases the value of ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{ASL})|$ exceeds 10 times;
- usually d'Hondt method favors large beneficiaries stronger than the QDLD method favors the small ones. In case of $M = 6$, the value of ratio $|\overline{F_{a1}}(\text{d'H})/\overline{F_{a1}}(\text{QDLD})|$ is of 91.2 times at $n = 4$ and of 2.25 times at $n = 5$.

References

[1] M.L. Balinski and H.P. Young, *Fair Representation: Meeting the Ideal of One Man, One Vote*, 2nd ed. Washington, DC, USA: Brookings Institution Press, 2001, 195 p. ISBN-10: 081570111X. ISBN-13: 978-0815701118.

[2] U. Kohler and J. Zeh, "Apportionment methods," *The Stata Journal*, vol. 12, no. 3, pp. 375–392, 2012.

[3] H.F. Niemeyer and A.C. Niemeyer, "Apportionment Methods," *Math. Social Sci.*, vol. 56, no. 2, pp. 240–253, 2008.

[4] M. Gallagher, "Proportionality, Disproportionality and Electoral Systems," *Electoral Studies*, vol. 10, no. 1, pp. 33–51, 1991.

[5] A. Karpov, "Measurement of disproportionality in proportional representation," *Mathematical and Computer Modeling*, vol. 48, pp. 1421–1438, 2008.

[6] K. Benoit, "Which Electoral Formula Is the Most Proportional? A New Look with New Evidence," *Political Analysis*, vol. 8, no. 4, pp. 381–388, 2000.

[7] V. d'Hondt, *La Répresentation Proportionnelles des Partis par un Electeur*, Ghent, 1878.

[8] A. Marshall, I. Olkin, and F. Pukelsheim, "A majorization comparison of apportionment methods in proportional representation," *Social Choice Welfare*, vol. 19, pp. 885–900, 2002.

[9] A. Sorescu, C. Pirvulescu et al. *Electoral systems*. Bucharest: Pro Democratia, 2006, 54 p. (in Romanian)

[10] E. Huntington, "A new method of apportionment of representatives," *Quart. Publ. Amer. Stat. Assoc*, vol. 17, pp. 859–1970, 1921.

[11] F. Pukelsheim, *Proportional Representation: Apportionment Methods and Their Applications*, Springer, 2014.

[12] M.L. Balinski, H.P. Young, "The Webster method of apportionment," *Proc. Natl. Acad. Sci. USA*, vol. 77, no. 1, pp. 1–4, 1980.

[13] I. Bolun, "A criterion for estimating the favoring of beneficiaries in apportionments," in *Workshop on Intelligent Informatition Systems, Proc. WIIS-2020, December 04-05, 2020*, (Chisinau), 2020, pp. 33–41.

[14] A.W. Marshall, I. Olkin, *Inequalities: Theory of majorization and its applications*, New York: Academic Press, 1979.

[15] I. Bolun, "Favoring of multioptional decisions options," in *Mathematical modeling, optimization and information technologies: intern. sc. confer., March 22-25, 2016. Ed. 5, Vol. I*, Chisinau: ATIC, 2016, pp. 35–45. (in Romanian)

[16] I. Bolun, "Total favoring in proportional apportionments," *Journal of Engineering Science*, vol. XXVIII, no. 1, pp. 47–60, 2021.

[17] I. Bolun, "Characterization of some apportionment methods," *Journal of Engineering Science*, vol. XXVI, no. 4, pp. 23–44, 2019.

Ion Bolun,

Received July 14, 2021
Revised version February 26, 2022
Accepted March 17, 2022

Technical Universty of Moldova
Studentilor, 9/7, Chisinau, Moldova
Phone: +373 22509908
E-mail: ion.bolun@isa.utm.md

Quadruplet loss and SqueezeNets for Covid-19 detection from Chest-X rays

Pranshav Gajjar, Naishadh Mehta, Pooja Shah

Abstract

The Coronavirus Pandemic triggered by SARS-CoV-2 has wreaked havoc on the planet and is expanding exponentially. While scanning methods, including CT scans and chest X-rays, are commonly used, artificial intelligence implementations are also deployed for COVID-based pneumonia detection. Due to image biases in X-ray data, bilateral filtration and Histogram Equalization are used followed by lung segmentation by a U-Net, which successfully segmented 83.2% of the collected dataset. The segmented lungs are fed into a Quadruplet Network with SqueezeNet encoders for increased computational efficiency and high-level embeddings generation. The embeddings are computed using a Multi-Layer Perceptron and visualized by T-SNE (T-Distributed Stochastic Neighbor Embedding) scatterplots. The proposed research results in a 94.6% classifying accuracy which is 2% more than the baseline Convolutional Neural Network and a 90.2% decrease in prediction time.

Keywords: COVID-19, Deep Learning applications, Lung Segmentation, X-Rays-based prediction

MSC 2020: 68R10, 68Q25, 05C35, 05C05.

1 Introduction

The rampant increase in Covid-19 caused by Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) [1] has induced worldwide trauma. With conventional and limited testing criteria resulting in false negatives, [2] and repeated testing. This paper proposes a similarity learning implementation to accelerate coronavirus detection.

©2022 by CSJM; Pranshav Gajjar, Naishadh Mehta, Pooja Shah
doi:10.56415/csjm.v30.12

The model can be used as a screening platform for RT-PCR tests [3], quickening covid detection and streamlining the process. Image biases caused due to a variety of different X-ray apparatus in the publicly available datasets are avoided by using Histogram Equalization and U-Net-based Chest segmentation [4]. The image biases consist of various insignificant textual data on images along with varying contrast values which can hinder training and feature learning. The sample images which show these imbalances are mentioned below in Figure 1.

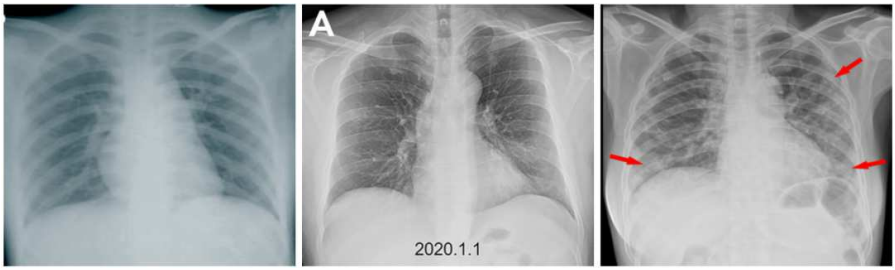


Figure 1. The first image contains a different color balance, the second image illustrates textual data and the third image carries various insignificant symbols that might hinder training

The proposed model is a Siamese Network [5] with SqueezeNet-based [6] vector generators, trained on Quadruplet Loss [7] which is used to procure high-level embeddings. The encoder architecture is kept as a vanilla SqueezeNet due to the lightweight nature, minimal weight sizes, and significantly faster prediction rates when compared to AlexNet or similar mainstream deep architectures [6]. The embeddings are further computed using an MLP (Multi-layered Perceptron) [8] and visualized by the T-SNE algorithm (T-distributed Stochastic Neighborhood Embedding) [9]. The proposed method outperformed a baseline CNN (Convolutional Neural Network) [10] in classifying segmented lung images into three groups (COVID-19 pneumonia, Normal Cases, Other Viral and Bacterial pneumonia) with an overall classifying accuracy of 94.6%, and gave superlative computational results like an 89.8% decrease in prediction time.

2 Related Work

Many attempts have been made for accurate classification of COVID-19 Pneumonia from body scans, mainly using Computerized Tomography (CT) scans and Chest X-rays [4]. The paper [11] used a DeTraC (Decompose, Transfer, and Compose) Deep Convolutional Neural Network on Chest X-rays and achieved a classification accuracy of 93.1%. The paper [12] used a CNN-based architecture called CovXNet resulting in a multiclass percentage accuracy of 90.2 and a 97.4% accuracy for COVID19/Normal binary classification. The paper [13] used a GAN (Generative Adversarial Network) for image augmentation and Light-CovidNet architecture for X-ray classification resulting in a 96.97% mean accuracy. The paper [14] used a Truncated Inception Net on a COVID-19 X-ray dataset and obtained an accuracy of 99.92% with an AUC of 1. The paper [15] designed a fuzzy strategy known as output Neuron Holding, which modifies the twice Transfer Learning technique. They used Layer-wise Relevance Propagation (LRP) to produce heat maps to help us understand how the models work. The paper [4] pointed out the complication of image biases caused due to a diversity of X-ray machines across the globe. The networks trained on publicly available datasets learned the image biases as a classification feature instead of COVID-based Pneumonia features causing fallacious real-time results. Hence, Lung segmentation is recommended and used.

3 Methodology

Total 2697 X-rays images are obtained by subsetting two databases, for COVID-19-based pneumonia [16] and for normal and other pneumonia [17]. The X-rays images of lungs undergo U-Net-based lung segmentation for image bias avoidance and are further classified using a SqueezeNet-based quadruplet loss model and an MLP. The proposed model and baselines are trained by identical 80:20 train-test splits, for an unbiased comparison. The Grayscale Images undergo bilateral filtration to enhance image quality and histogram equalization to nullify contrast-based biases. Preprocessed images have an array shape of 256x256 and are fed into a U-Net for lung segmentation purposes.

The segmentation model is trained on the famous JSRT [18] and Montgomery dataset [19] which contains non-pneumonia chest X-rays and the ground truth Lung masks. Due to the dataset constraint for COVID-19 X-rays, unavailability of a COVID-based segmentation dataset, and image clarity uncertainties, only 83.2% of images are successfully segmented. The entire process of Lung segmentation and image preprocessing is shown below in Figure 2.

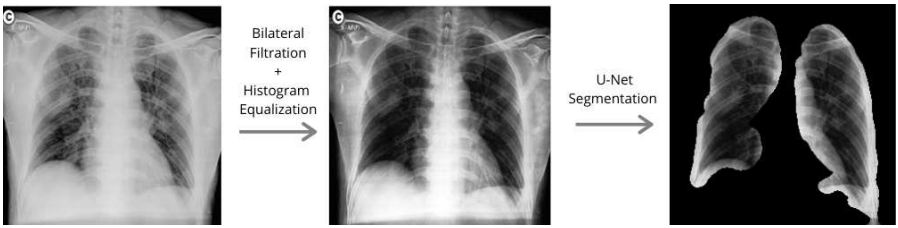


Figure 2. Sample flow of X-ray preprocessing for a segmented output

The segmented lung set is used to generate random quadruplets containing an anchor image of a particular class, a positive image with the same class, and two negative images depicting different classes. The quadruplets are fed into a Siamese network with Quadruplet Loss and four SqueezeNets, which have shared weights and are implemented for vector generation. The loss function follows the original paper [7] with the hyperparameters 'alpha' and 'beta', fine-tuned as 0.2. The model pipeline for computing Quadruplet Loss and similarity learning is mentioned below in Figure 3.

The SqueezeNets contain multiple Fire Modules and Pooling layers along with a Squeeze Ratio [6] of 0.125, which, when trained for similarity learning, generates a memory-efficient embedding space, which can be further used for pneumonia classification. The softmax layer is removed and a dense layer is added for embedding generation and similarity learning. The embeddings obtained from the SqueezeNet have a dimensionality of 256. They are further fed into a three-layered perceptron, which classifies the embeddings by computing a probabilistic distribution of the four pneumonia classes.

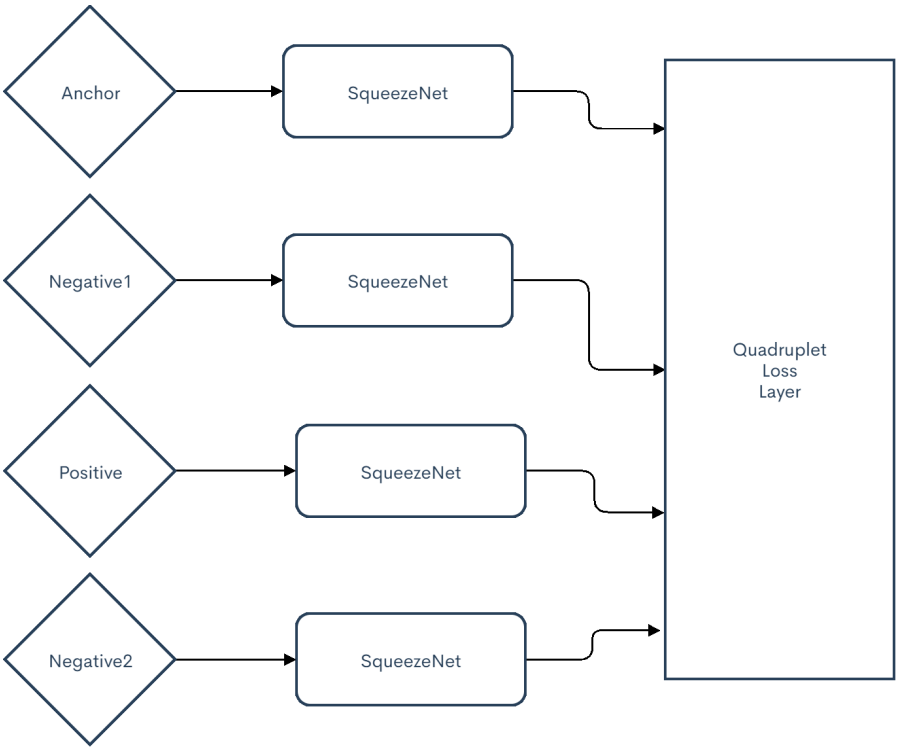


Figure 3. Data flow for the quadruplet loss network

4 Results and Discussion

To justify the use of proposed methodologies, a Convolution Neural Network (CNN) is used as a baseline. The model contains four convolutional blocks, and each block contains a convolutional layer with $2\hat{n}$ filters and a Max-Pooling layer with a pooling window of 2,2. The first block contains 32 filters followed by 64 and 128 convolutional units. The outputs are flattened and fed into a softmax layer for a probabilistic distribution of classes. The model is trained on the Cross-Entropy loss [20] function with a learning rate of 10^{-3}.

All the mentioned approaches are trained and benchmarked on a singular Google Colaboratory GPU accelerated runtime [21]. This en-

sures a safe and unbiased comparative study. The framework called Keras [22] is used for the deployment of all the mentioned deep learning algorithms. The proposed model gave a classifying accuracy of 94.6%, outperforming the baseline CNN by '2%'. The prediction time for the entire pipeline averaged 0.245 seconds for 449 segmented X-rays, which was 10.2 times faster than the baseline. The use of similarity learning is also deemed successful by observing the T-SNE scatter plots as the intra-class distance is minimized and the inter-class distance is maximized.

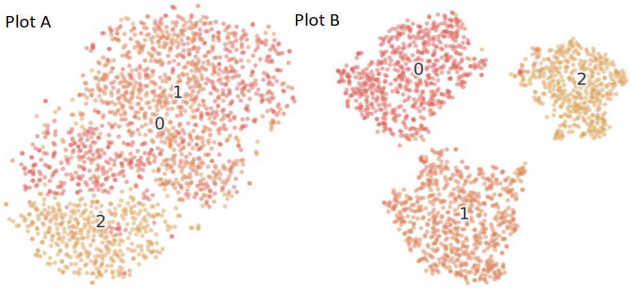


Figure 4. T-SNE Scatter plots, Plot A contains unaltered testing data whereas Plot B contains the high-level embeddings generated by the SqueezeNet Encoder. Here, '0', '1', and '2' represent 'Covid-19 pneumonia', 'other pneumonia' and 'normal cases' respectively

5 Conclusion and Future Work

The paper proposed a Quadruplet Loss approach with SqueezeNet-based vector generation for automated COVID-19 detection from chest X-rays. The said methodologies were able to successfully classify segmented lungs with an accuracy of 94.6% and an extremely low prediction time averaging at 5.45 x (10^-4) seconds per image. The model outperformed a baseline CNN with an increase in classification accuracy of 2% and faster prediction times with a factor of 10.2.

For the upcoming future, we will test the robustness of the algorithm, implement multiple Encoder Architectures and work on a superior lung segmentation method for pneumonia patients which is independent of dataset constraints.

References

[1] A. Pivato, I. Amoruso, G. Formenton, F. Di Maria, T. Bonato, S. Vanin, A. Marion, and T. Baldovin, "Evaluating the presence of SARS-CoV-2 RNA in the particulate matters during the peak of COVID-19 in Padua, northern Italy," *Science of the Total Environment*, vol. 784, p. 147129, 2021.

[2] C. P. West, V. M. Montori, and P. Sampathkumar, "COVID-19 Testing: The Threat of False-Negative Results," in *Mayo Clinic Proceedings*, vol. 95, no. 6. Elsevier, 2020, pp. 1127–1129.

[3] P. D. Siebert, "RT-PCR Methods and Applications," in *Molecular Diagnosis of Infectious Diseases*. Springer, 1998, pp. 29–53.

[4] E. Tartaglione, C. A. Barbano, C. Berzovini, M. Calandri, and M. Grangetto, "Unveiling COVID-19 from CHEST X-ray with Deep Learning: A Hurdles Race with Small Data," *International Journal of Environmental Research and Public Health*, vol. 17, no. 18, p. 6933, 2020.

[5] I. Melekhov, J. Kannala, and E. Rahtu, "Siamese network features for image matching," in *2016 23rd International Conference on Pattern Recognition (ICPR)*. IEEE, 2016, pp. 378–383.

[6] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5 MB model size," *arXiv preprint arXiv:1602.07360*, 2016.

[7] W. Chen, X. Chen, J. Zhang, and K. Huang, "Beyond Triplet Loss: A Deep Quadruplet Network for Person Re-Identification," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 403–412.

[8] T. Kristensen, "A Multi-Layered Perceptron fingerprint idenfication system," in *2011 Third World Congress on Nature and Biologically Inspired Computing*. IEEE, 2011, pp. 491–497.

[9] G. C. Linderman, M. Rachh, J. G. Hoskins, S. Steinerberger, and Y. Kluger, "Efficient Algorithms for t-distributed Stochastic Neighborhood Embedding," *arXiv preprint arXiv:1712.09005*, 2017.

[10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017.

[11] A. Abbas, M. M. Abdelsamea, and M. M. Gaber, "Classification of COVID-19 in chest X-ray images using DeTraC deep convolutional neural network," *Applied Intelligence*, vol. 51, no. 2, pp. 854–864, 2021.

[12] T. Mahmud, M. A. Rahman, and S. A. Fattah, "CovXNet: A multi-dilation convolutional neural network for automatic COVID-19 and other pneumonia detection from chest X-ray images with transferable multi-receptive feature optimization," *Computers in biology and medicine*, vol. 122, p. 103869, 2020.

[13] M. A. Zulkifley, S. R. Abdani, and N. H. Zulkifley, "COVID-19 Screening Using a Lightweight Convolutional Neural Network with Generative Adversarial Network Data Augmentation," *Symmetry*, vol. 12, no. 9, p. 1530, 2020.

[14] D. Das, K. Santosh, and U. Pal, "Truncated inception net: COVID-19 outbreak screening using chest X-rays," *Physical and engineering sciences in medicine*, vol. 43, no. 3, pp. 915–925, 2020.

[15] P. R. Bassi and R. Attux, "A deep convolutional neural network for COVID-19 detection using chest X-rays," *Research on Biomedical Engineering*, pp. 1–10, 2021.

[16] A. A. Chung, "COVID-19 chest X-ray data initiative," 2020.

[17] D. S. Kermany, M. Goldbaum, W. Cai, C. C. Valentim, H. Liang, S. L. Baxter, A. McKeown, G. Yang, X. Wu, F. Yan *et al.*, "Identifying Medical Diagnoses and Treatable Diseases by Image-Based Deep Learning," *Cell*, vol. 172, no. 5, pp. 1122–1131, 2018.

[18] J. Shiraishi, S. Katsuragawa, J. Ikezoe, T. Matsumoto, T. Kobayashi, K.-i. Komatsu, M. Matsui, H. Fujita, Y. Kodera, and K. Doi, "Development of a Digital Image Database for Chest Radiographs With and Without a Lung Nodule Receiver Operating Characteristic Analysis of Radiologists' Detection of Pulmonary Nodules," *American Journal of Roentgenology*, vol. 174, no. 1, pp. 71–74, 2000.

[19] S. Jaeger, S. Candemir, S. Antani, Y.-X. J. Wáng, P.-X. Lu, and G. Thoma, "Two public chest X-ray datasets for computer-aided screening of pulmonary diseases," *Quantitative imaging in medicine and surgery*, vol. 4, no. 6, p. 475, 2014.

[20] A. Jamin and A. Humeau-Heurtier, "(Multiscale) Cross-Entropy Methods: A Review," *Entropy*, vol. 22, no. 1, p. 45, 2020.

[21] E. Bisong, *Building Machine Learning and Deep Learning models on Google Cloud Platform: A Comprehensive Guide for Beginners*. Apress, 2019.

[22] F. Chollet *et al.* (2015) Keras. [Online]. Available: https://github.com/fchollet/keras

Pranshav Gajjar, Naishadh Mehta, Pooja Shah

Received May 9, 2021
Revised version March 1, 2022
Accepted March 1, 2022

Pranshav Gajjar
Institute of Technology, Nirma University
Ahmedabad, Gujarat, India
E–mail: 19bce060@nirmauni.ac.in

Naishadh Mehta
Institute of Technology, Nirma University
Ahmedabad, Gujarat, India
E–mail: 19mced07@nirmauni.ac.in

Pooja Shah
Institute of Technology, Nirma University
Ahmedabad, Gujarat, India
E–mail: pooja.shah@nirmauni.ac.in

The Domination Parameters on a kind of the regular honeycomb structure

Fateme Movahedi, Kok Keong Choong,
Mohammad Hadi Akhbari

Abstract

The honeycomb mesh, based on hexagonal structure, has enormous applications in chemistry and engineering. A major challenge in this field is to understand the unique properties of honeycomb structures, which depend on their properties of topology.

One of the important concepts in graph theory is the domination number which can be used for network control and monitoring. In this paper, we investigate the domination number of the honeycomb network. For this purpose, the domination number, the total domination number, the independent domination number, the connected domination number and the doubly connected domination number of the honeycomb are obtained. Finally, in some honeycomb structures of real models, we obtain the exact amount of these parameters.

Keywords: Honeycomb structure, Total domination number, Independent domination number, Connected domination number, Doubly connected domination number.

MSC 2010: 05C69, 97R20.

1 Introduction

The honeycomb mesh is a network that is convenient for modeling and designing some engineering models and/or chemical structures. Using honeycomb structures based on the geometry of a honeycomb in engineering sciences allows minimizing the amount of used material to reach minimal weight and minimal material cost. The geometry of

©2022 by CSJM; F. Movahedi, K. K. Choong, M. H. Akhbari
doi:10.56415/csjm.v30.13

honeycomb structures can vary widely but the common feature of all such structures is a set of hollow cells formed between thin vertical walls. The cells are often columnar and hexagonal in shape [1]. The honeycomb networks have also been recognized as crucial as a representation of benzenoid hydrocarbons in chemistry. These networks had found widespread applications in various fields such as architecture, mechanical engineering, chemistry, transportation, nanofabrication and biomedicine [2].

A major challenge is to understand the unique properties of honeycomb structures based on the properties of their topologies. So, the study on the properties of the topology of honeycomb structures has been considered. Honeycomb networks are better in terms of degree, diameter, and total number of links, cost, and bisection width than mesh connected planar graphs [3]. Stojmenovic [4] has studied the topological properties of honeycomb networks, routing in honeycomb networks and honeycomb torus networks.

In [5], the degree diameter problem on honeycomb networks is studied. Manuel et al. determined the minimum metric bases for hexagonal and honeycomb networks [6]. In [7], an approximation algorithm is proposed to obtain the harmonious chromatic number of honeycomb. An algorithm for finding a perfect packing of honeycomb networks is proposed in [8].

One of the important and well-known concepts in graph theory is the study of the dominating sets in a graph. The studies of domination set are important in the control of engineering systems. The dominating set has already been applied to the control or design of different types of engineering systems, which include mobile computing [9], computer communication networks [10], computational biology and biomedical analysis [11].

Recall that for a simple graph G with the vertices set V and the edges set E, the dominating set D of the vertices subset of the graph G is such that every vertex is either in D or adjacent to a vertex in D. Domination in graphs has been extensively researched as one of the branches in graph theory and has many applications in science and technology [12]. A survey of several advanced topics of domination is given in the book by Haynes et al. [13]. The domination number of

graph G, denoted by $\gamma(G)$, is the minimum size of a dominating set of G.

The minimum dominating set is classified as NP-Completeness and in general cannot be solved exactly in polynomial time [14], [15]. It means that there is no theoretically efficient algorithm that finds the exact smallest dominating set for a given graph. Therefore, many heuristic and approximation algorithms are proposed to find the minimum dominating set of a graph. Some proposed algorithms for selecting the minimum dominating set of a given graph can be found in [16]–[18]. In this paper, we determine the minimum dominating set of a honeycomb network and obtain the exact formula for the domination number based on the parameters of the honeycomb structure.

There are several parameters of domination that can be used to simulate some properties of networks and chemical graphs [19]–[21]. A dominating set D is a total dominating set of G if every vertex of the graph is adjacent to at least one vertex in D. The total domination number of G, denoted by $\gamma_t(G)$ is the minimum size of a total dominating set of G. A dominating set D is called an independent dominating set if D is an independent set. The independent domination number of G denoted by $\gamma_i(G)$ is the minimum size of an independent dominating set of G. Obviously, for each graph G, $\gamma(G) \leq \gamma_i(G)$ [13]. The subset D of the set of vertices $V(G)$ is a connected dominating set in G if D is a dominating set and the subgraph induced by D is connected. The minimum cardinality of any connected dominating set in G is called the connected domination number of G and it is denoted by $\gamma_c(G)$ [22]. A set $D \subseteq V(G)$ is a doubly connected dominating set of G if it is dominating and both induced subgraphs D and $V(G) \setminus D$ are connected. The cardinality of a minimum doubly connected dominating set of G is the doubly connected domination number of G and is denoted by $\gamma_{cc}(G)$ [23].

In this paper, we obtain the total domination number, the independent domination number, the connected domination number and the doubly connected domination number of a given honeycomb network as one of the properties of their topologies. In Section 3, applied examples based on the modeling of honeycomb structures are included to obtain the validity and applicability of the domination parameters.

2 Main Results

In this section, we consider the kind of regular honeycomb structure called the general structure [24]. This structure of honeycomb contains an array of hollow cells with the number of $n \geq 2$ cells that are formed between $k \geq 1$ thin vertical walls of the cells, which have a hexagonal shape. So, k is an odd number (see Figure 1).

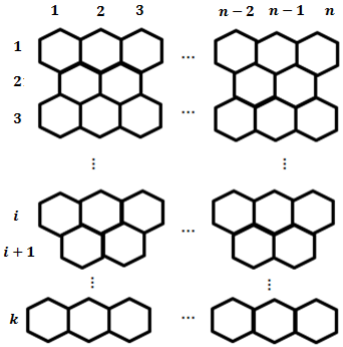


Figure 1. Honeycomb structure with n cells in rows and k cells in columns.

However, the configuration of Figure 1 can be changed with different geometric transformations [25] and structure graph HC is shown as Figure 2.

According to Figure 1, the number of the vertices of this honeycomb structure (HC) is $(2n + 1)(k + 1)$. The vertex degrees are 2 and 3 such that $2(n - 1) + (2n - 1)(k - 1)$ vertices have degree 3, and the remained vertices have degree 2. According to Figure 2, in any subgraph G_i for $1 \leq i \leq \lceil \frac{k}{2} \rceil$, vertices are labeled as $\{1, 2, \ldots, 2n + 1\}$ in path P_1 and $\{2n + 2, 2n + 3, \ldots, 4n + 2\}$ in path P_2. Also, in any subgraph H_i, for $1 \leq i \leq \lfloor \frac{k}{2} \rfloor$, vertices are labeled as $\{2n + 3, 2n + 4, 2n + 5, \ldots, 4n + 1, 2, 3, 4, 5, \ldots, 2n - 1\}$.

We obtain the number of domination parameters of the graph HC. Also, the minimum set of these parameters is determined.

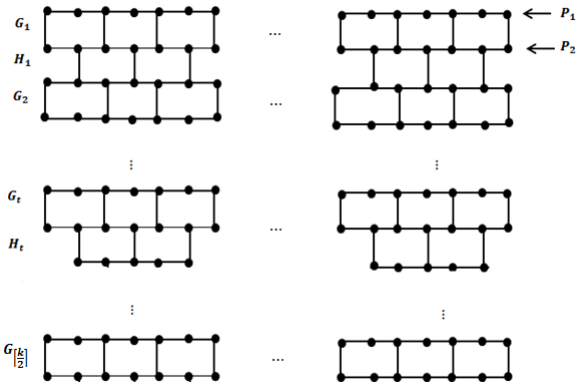


Figure 2. Graph HC obtained from Figure 1.

Theorem 1. *Let the graph HC be a honeycomb structure that contains n hexagonal cells in rows and k hexagonal cells in columns for $n \geq 2$ and $k > 1$. Then*

$$\gamma(HC) = (n+1)\left\lceil \frac{k}{2} \right\rceil.$$

Proof. Let D be the dominating set of graph HC that is shown in Figure 2. We consider subgraphs G_i of HC for $1 \leq i \leq \lceil \frac{k}{2} \rceil$. If D_i is the dominating set of graph G_i, then it is easy to see that $D = \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} D_i$. So, one can select the set D_i as follows:
Case 1: If n is odd, then

$$D_i = \{1, 5, 9, 13, \ldots, 2n-1, 2n+4, 2n+8, 2n+12, \ldots, 4n-2, 4n+2\},$$

such that $|D_i| = n+1$.
Case 2: If n is even, then

$$D_i = \{1, 5, 9, 13, \ldots, 2n-3, 2n+1, 2n+4, 2n+8, \ldots, 4n-4, 4n\},$$

and $|D_i| = n+1$.

Therefore, $|D| = (n+1)\lceil \frac{k}{2} \rceil$.

Assume that there exists a dominating set D of the graph HC with $|D| \leq (n+1)\lceil \frac{k}{2} \rceil - 1$. According to the structure of the graph HC

shown in Figure 2, at least one of the vertices $\{1, 2n+1\}$ and one of the vertices $\{2n+2, 4n+2\}$ in any subgraph G_i for $1 \leq i \leq \lceil \frac{k}{2} \rceil$ must be selected in D. Because otherwise, the set D must contain the vertices $\{2, 2n, 2n+3, 4n+1\}$, where instead of two vertices, we have to select 4 vertices. Therefore, at least $2\lceil \frac{k}{2} \rceil$ vertices of the set D have the degree 2. So, the number of vertices of degree 3 is at most

$$(n+1)\left\lceil \frac{k}{2} \right\rceil - 1 - 2\left\lceil \frac{k}{2} \right\rceil = (n-1)\left\lceil \frac{k}{2} \right\rceil - 1.$$

Since any vertices with degree 2 in D dominate two vertices in a graph HC and any vertices with degree 3 dominate three vertices, thus, the number of vertices of HC dominated by D is at most $4n\lceil \frac{k}{2} \rceil - 4$. With a simple computation, for $n \geq 2$ and $k > 1$, we can obtain $(2n+1)(k+1) > 4n\lceil \frac{k}{2} \rceil - 4$. So, it is a contraction and we have $\gamma(HC) = (n+1)\lceil \frac{k}{2} \rceil$. □

Theorem 2. *Let the graph HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $n \geq 2$ and $k > 1$. Then*

$$\gamma_t(HC) = 2(n+1) + (k-1)n.$$

Proof. Let TD be the total dominating set of the graph HC. According to Figure 2 and by considering subgraphs G_1 and $G_{\lceil \frac{k}{2} \rceil}$, one can select the total dominating sets TD_1 and $TD_{\lceil \frac{k}{2} \rceil}$ as the following sets on the paths P_1 and P_2 from subgraphs G_1 and $G_{\lceil \frac{k}{2} \rceil}$, respectively.
Case a) If n is even, then

$$TD_1 = \big\{2, 3, 6, 7, 10, 11, 14, 15, \ldots, 2n-2, 2n-1, 2n\big\},$$

with $|TD_1| = n+1$ and

$$TD_{\lceil \frac{k}{2} \rceil} = \big\{2n+3, 2n+4, 2n+7, 2n+8, \ldots, 4n-1, 4n, 4n+1\big\},$$

where $\big|TD_{\lceil \frac{k}{2} \rceil}\big| = n+1$. Also, the total dominating set TD_i from subgraphs H_i, $1 \leq i \leq \lfloor \frac{k}{2} \rfloor$, is considered as follows:

$$TD_i = \big\{2, 4, \ldots, 2n, 2n+3, 2n+5, \ldots, 4n+1\big\},$$

with $|TD_i| = 2n$.

Thus, we can consider the set $TD = \bigcup_{i=1}^{\lfloor \frac{k}{2} \rfloor} TD_i \bigcup \{TD_1, TD_{\lceil \frac{k}{2} \rceil}\}$ as the total dominating set for the graph HC that $|TD| = 2(n+1)+2\lfloor \frac{k}{2} \rfloor n$. Since k is odd, then $|TD| = 2(n+1) + (k-1)n$.

Case b) If n is odd, we select

$$TD_1 = \{2, 3, 6, 7, 10, 11, 14, 15, \ldots, 2n-2, 2n, 2n+1\},$$

and

$$TD_{\lceil \frac{k}{2} \rceil} = \{2n+3, 2n+4, 2n+6, 2n+7, \ldots, 4n+1, 4n+2\},$$

where $|TD_1| = |TD_{\lceil \frac{k}{2} \rceil}| = n+1$. For $1 \leq i \leq \lfloor \frac{k}{2} \rfloor$, we consider

$$TD_i = \{2, 4, \ldots, 2n, 2n+3, 2n+5, \ldots, 4n+1\}.$$

Therefore, $|TD| = 2(n+1) + (k-1)n$. Thus, we have $\gamma_t(HC) \leq 2(n+1) + (k-1)n$.

Assume that the set TD be the total dominating set of the graph HC and $|TD| \leq 2(n+1) + (k-1)n - 1$. According to the structure of the graph HC and the degrees of vertices of the graph, there are the following cases.

Case 1: There are $4\lceil \frac{k}{2} \rceil$ vertices of degree 2 such that at least any two vertices are adjacent to each other and the remained vertices of TD have degree 3. The number of vertices of degree 3 is $2(n+1) + (k-1)n - 1 - 4\lceil \frac{k}{2} \rceil$. Since any vertex of degree 2 dominates at least one vertex of the graph HC, the number of dominated vertices of HC is equal to $8\lceil \frac{k}{2} \rceil$.

Also, the vertices of degree 3 dominate at least one vertex of the graph HC; the number of them is as follows:

$$2\Big(2(n+1) + (k-1)n - 1 - 4\lceil \frac{k}{2} \rceil\Big).$$

Therefore, the number of dominated vertices of HC is as follows

$$2\Big(2(n+1) + (k-1)n - 1\Big).$$

Since the number of vertices of the graph HC is $(2n+1)(k+1)$, some vertices of the graph HC cannot dominate by TD. Therefore, it is a contradiction that TD is the total dominating set.

Case 2: Assume that the set TD contains $2(n+2)+4\Big(\lceil\frac{k}{2}\rceil-2\Big)$ vertices of degree 2 such that in the neighborhood of its any vertex exists at least one vertex of degree 3. So, the number of vertices of degree 3 of the graph HC is $(k-1)n-4\lceil\frac{k}{2}\rceil+5$ in TD. Since any vertex of degree 2 and 3 at least dominates one vertex of HC, the number of dominated vertices of the graph by TD is $2(k-1)n+4(n+2)-6$. For $n\geq 2$ and $k\geq 1$, $(2n+1)(k+1) > 2(k-1)n+4(n+2)-6$. Thus, at least one vertex of honeycomb HC cannot dominate by vertices of TD and it is a contradiction.

Case 3: If all of the vertices of degree 3 are in the set TD. Then the number of them is $4(n-1)+2n\lceil\frac{k}{2}\rceil$ and the remained vertices of the set TD have the degree 2 with size $2(n+1)+(k-1)n-1-4(n-1)-n\lceil\frac{k}{2}\rceil$. For $n\geq 2$ and $k\geq 1$, one can obtain that the number of degree 2 in the set TD is negative by a simple calculation. So, it is a contradiction in this case.

Case 4: Let TD contains $2n+4\lceil\frac{k}{2}\rceil$ vertices of HC such that one of two vertices of any two adjacent vertices in TD has degree 2 and the other vertex has degree 3. The number of remaining vertices of TD in HC equals $(k-1)n-4\lceil\frac{k}{2}\rceil-1$. Since $(k-1)n-4\lceil\frac{k}{2}\rceil-1<0$ for $n\geq 2$ and $k\geq 1$, thus this case is a contradiction.

Therefore, in all of the above cases and similar cases, for the total dominating set with $|TD|\leq 2(n+1)+(k-1)n-1$, we obtain a contradiction. So, the result follows. □

Theorem 3. *Let HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $n\geq 2$ and $k>1$. Then*

$$\gamma_i(HC)=(n+1)\lceil\frac{k}{2}\rceil.$$

Proof. Similar to Theorem 1, one can obtain the independent dominating set ID of HC as follows.

Let ID_i be the independent dominating set of the graph G_i shown in Figure 2. For the two following cases, we get

Case 1: If n is even, then we can choose

$$ID_i = \big\{1, 5, 9, 13, \ldots, 2n-3, 2n+1, 2n+4, \ldots, 4n-4, 4n\big\},$$

Case 2: If n is odd, then

$$ID_i = \big\{1, 5, 9, 13, \ldots, 2n-1, 2n+4, 2n+8, \ldots, 4n-2, 4n+2\big\}.$$

For both cases, $|ID_i| = n+1$, where $1 \leq i \leq \lceil \frac{k}{2} \rceil$. Therefore, we have $ID = \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} ID_i$ and $|ID| = (n+1)\lceil \frac{k}{2} \rceil$. Since the set ID is a dominating and independent set, then $\gamma_i(HC) \leq \lceil \frac{k}{2} \rceil (n+1)$.

On the other hand, using Theorem 1,

$$\left\lceil \frac{k}{2} \right\rceil (n+1) = \gamma(HC) \leq \gamma_i(HC) = \left\lceil \frac{k}{2} \right\rceil (n+1).$$

Therefore, the result completes. □

Theorem 4. *Let HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $n \geq 4$ and $k > 1$. Then*

$$\gamma_c(HC) = 2\left\lceil \frac{k}{2} \right\rceil (2n-3) + 1.$$

Proof. Let CD be the connected dominating set of the graph HC. One can select the connected dominating set CD as follows.

Case 1: Assume that n is even. According to Figure 2, we consider all of the vertices from P_1 in subgraph G_1 except $\{1, 2n+1\}$ in CD. Thus, the number of these vertices is $2n-1$. The remained vertices selected from P_2 in subgraph G_1 are as follows:

$$Big\{2n+3, 2n+4, \ldots, 2n + \left\lceil \frac{2n+1}{2} \right\rceil - 1, 2n + \left\lceil \frac{2n+1}{2} \right\rceil + 3,$$
$$2n + \left\lceil \frac{2n+1}{2} \right\rceil + 4, \ldots, 4n+1\Big\},$$

where the number of these vertices is $2n-4$.

For $2 \leq i \leq \lceil \frac{k}{2} \rceil$, we consider the following vertices of subgraphs G_i in the set CD

$$\Big\{2, 3, 4, \ldots, \left\lceil \frac{2n+1}{2} \right\rceil - 1, \left\lceil \frac{2n+1}{2} \right\rceil + 2, \left\lceil \frac{2n+1}{2} \right\rceil + 3, \ldots, 2n,$$
$$2n+3, 2n+4, \ldots, 2n + \left\lceil \frac{2n+1}{2} \right\rceil, 2n + \left\lceil \frac{2n+1}{2} \right\rceil + 3, \ldots, 4n+1\Big\},$$

where the number of these vertices is $4n-6$.

So, $|CD| = (2n-1)+(2n-4)+\Big(\Big\lceil\frac{k}{2}\Big\rceil-1\Big)(4n-6) = 2\Big\lceil\frac{k}{2}\Big\rceil(2n-3)+1$.

Case 2: Let n be odd. Similar to case 1, select the following vertices of subgraphs G_i for $1 \le i \le \lceil\frac{k}{2}\rceil$:

In path P_1 of subgraph G_1, select all of the vertices except $\{1, 2n+1\}$ in CD.

In path P_2 of subgraph G_1, we consider the following vertices:

$$\Big\{2n+3, 2n+4, \ldots, 2n+\Big\lceil\frac{2n+1}{3}\Big\rceil+1, 2n+\Big\lceil\frac{2n+1}{3}\Big\rceil+5,$$
$$2n+\Big\lceil\frac{2n+1}{3}\Big\rceil+6, \ldots, 4n+1\Big\}.$$

For $2 \le i \le \lceil\frac{k}{2}\rceil$, we consider the following vertices of subgraphs G_i in the set CD:

$$\Big\{2, 3, 4, \ldots, \Big\lceil\frac{2n+1}{3}\Big\rceil+1, \Big\lceil\frac{2n+1}{3}\Big\rceil+4, \ldots, 2n, 2n+3, 2n+4, \ldots,$$
$$2n+\Big\lceil\frac{2n+1}{3}\Big\rceil+2, 2n+\Big\lceil\frac{2n+1}{3}\Big\rceil+4, \ldots, 4n+1\Big\}.$$

So, $|CD| = 2\Big\lceil\frac{k}{2}\Big\rceil(2n-3)+1$. Thus, we have $\gamma_c(HC) \le 2\Big\lceil\frac{k}{2}\Big\rceil(2n-3)+1$.

Let CD be the connected dominating set, where $|CD| \le 2\Big\lceil\frac{k}{2}\Big\rceil(2n-3)$. If the set CD contains only vertices of degree 2 or degree 3, then it contradicts the definition of the connected dominating set for the set CD. Thus, the vertices in CD have both degrees 2 and 3.

Let CD contain at least $2\lceil\frac{k}{2}\rceil$ vertices of degree 2, and the remained vertices are of degree 3. Thus, $2\Big\lceil\frac{k}{2}\Big\rceil(2n-4)$ vertices of degree 3 are dominated by some vertices of the graph HC.

According to the structure HC and the definition of the connected dominating set CD in HC, any vertex with degree 2 dominates at least another vertex such that one of its adjacent vertices must be in CD. So, the number of dominated vertices in HC by these vertices is $2\Big\lceil\frac{k}{2}\Big\rceil$. Since CD is the connected set, any vertex with degree 3 dominates at least two vertices of a graph HC such that at least one of its adjacent

vertices must be in CD. Therefore, the number of dominated vertices in HC is at most

$$2\left\lceil\frac{k}{2}\right\rceil + 2\left\lceil\frac{k}{2}\right\rceil(2n-4).$$

Using easy computing, one can obtain that the number of dominated vertices in graph HC is less than the number of vertices in $V \setminus D$. So, it is a contradiction. Therefore, the result is complete. □

Theorem 5. *Let HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $k > 1$.*

(i) If $n = 2$, then

$$\gamma_c(HC) = 3\left\lceil\frac{k}{2}\right\rceil,$$

(ii) If $n = 3$, then

$$\gamma_c(HC) = 8\left\lceil\frac{k}{2}\right\rceil + 10.$$

Proof. (i) Assume that $n = 2$ and $k > 1$. Let CD be the connected dominating set of HC. One can select the vertices of the set CD_i of subgraphs G_i for $1 \leq i \leq \lceil\frac{k}{2}\rceil$ as follows:

$$CD_i = \{2, 3, \ldots, 2n\}.$$

Since $CD = \bigcup_{i=1}^{\lceil\frac{k}{2}\rceil} CD_i$ is the connected dominating set of the graph HC, then $|CD| = 3\left\lceil\frac{k}{2}\right\rceil$. Therefore, $\gamma_c(HC) = 3\left\lceil\frac{k}{2}\right\rceil$. Similar to Theorem 4 and the structure of the graph HC, it is easy to see that the connected dominating set CD has the minimum cardinality between the connected dominating set of HC. Thus, the result follows.

(ii) Similar to case (i) and the proof of Theorem 4, we select the connected domination set CD for the graph HC as follows. The vertices of subgraph G_1 and $G_{\lceil\frac{k}{2}\rceil}$ are considered as

$$CD_1 = CD_{\lceil\frac{k}{2}\rceil} = \{2, 3, 4, 5, 6, 9, 10, 12, 13\}.$$

For $2 \leq i \leq \lceil \frac{k}{2} \rceil - 1$, we select the vertices of subgraphs G_i

$$CD_i = \{2, 3, 5, 6, 9, 10, 12, 13\}.$$

Since $CD = \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} CD_i$, we get $|CD| = 2 \times 9 + 8\Big(\Big\lceil \frac{k}{2} \Big\rceil - 1\Big)$. □

Theorem 6. *Let HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $n \geq 3$ and $k > 1$. Then*

$$\gamma_{cc}(HC) = k(2n+1) - 4\Big\lceil \frac{k}{2} \Big\rceil + 9.$$

Proof. Let CCD be the doubly connected dominating set of the graph HC. One can select the set CCD such that all of the vertices of HC are selected in CCD except for the vertices sets of subgraphs G_i for $1 \leq i \leq \lceil \frac{k}{2} \rceil$ as follows: in subgraph G_1, the set $\{3, 4, 2n+4, 2n+5\}$; in subgraph $G_{\lceil \frac{k}{2} \rceil}$, the set $\{4, 5, 6, \ldots, 2n-1\}$; in subgraph G_i, the set $\{4, 5, 2n+5, 2n+6\}$ for $2 \leq i \leq \lceil \frac{k}{2} \rceil - 1$.

Therefore,

$$|CCD| = (2n+1)(k+1) - \Big(4\Big\lceil \frac{k}{2} \Big\rceil + 2n - 8\Big) = k(2n+1) - 4\Big\lceil \frac{k}{2} \Big\rceil + 9.$$

So, $\gamma_{cc}(HC) \leq k(2n+1) - 4\Big\lceil \frac{k}{2} \Big\rceil + 9$.

Let CCD be the doubly connected dominating set such that $\gamma_{cc}(HC) \leq k(2n+1) - 4\Big\lceil \frac{k}{2} \Big\rceil + 8$. Since CCD is the doubly connected domination set, then, by the structure of the graph HC, the vertices $\{1, 2n+1, 2n+2, 4n+2\}$ in any subgraph G_i for $1 \leq i \leq \lceil \frac{k}{2} \rceil$ must be selected in CCD. So, the number of vertices with degree 2 is at least $4\Big\lceil \frac{k}{2} \Big\rceil$. Since CCD is the connected set, then the set CCD contains the vertices $\{2, 2n, 2n+3, 4n+1\}$. Thus, the number of these vertices in CCD is at least $8\Big\lceil \frac{k}{2} \Big\rceil$. Similarly, the number of vertices with degree 3 is at most $k(2n+1) - 8\Big\lceil \frac{k}{2} \Big\rceil + 8$ in the set CCD such that at least one of its adjacent vertices is in CCD. Therefore, the number of these vertices is equal to $2k(2n+1) - 16\Big\lceil \frac{k}{2} \Big\rceil + 16$.

According to the above argument, the cardinality of CCD is at least $2k(2n+1) - 8\left\lceil \frac{k}{2} \right\rceil + 16$. By a simple calculation, for $n \geq 3$ and $k > 1$, the number of vertices in CCD is more than $k(2n+1) - 4\left\lceil \frac{k}{2} \right\rceil + 8$ that it is a contradiction. Therefore, the result completes. □

Theorem 7. *Let the graph HC be a honeycomb structure containing n hexagonal cells in rows and k hexagonal cells in columns for $n = 2$ and $k > 3$. Then*

$$\gamma_{cc}(HC) = 5k - 6\left\lceil \frac{k}{2} \right\rceil + 13.$$

Proof. Let CCD be the doubly connected dominating set of the graph HC for $n = 2$ and $k > 3$. We can select all of the vertices of HC except the following ones: in subgraph G_1, the set $\{7, 8\}$; in subgraph $G_{\lceil \frac{k}{2} \rceil}$, the set $\{2, 3\}$; in subgraph G_i, the set $\{1, 2, 3, 6, 7, 8\}$ for $2 \leq i \leq \lceil \frac{k}{2} \rceil - 1$.

Since the number of vertices of HC is equal to $5(k+1)$, then we have $|CCD| = 5k - 6\left\lceil \frac{k}{2} \right\rceil + 13$.

It is easy to see that the doubly connected dominating set CCD has the minimum cardinality between the doubly connected dominating set of the graph HC. Therefore, the result follows.

□

3 Illustrative examples

In this section, we study the domination number, the total domination number, the independent domination number, the connected domination number and the doubly connected domination number of two applied honeycomb models in engineering and chemistry.

We present a kind of the structure of hydrocarbon as Hexa-perihexabenzocoronene (HBC) that contains a central coronene molecule, with an extra benzene ring fused between each adjacent pair of rings around the periphery (see Figure 3). The HBC molecule is interesting to chemists because of its applications and structure [26]. In the following example, we obtain the domination parameters studied in this paper on the structure of HBC.

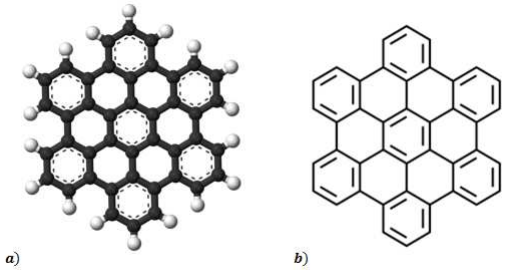


Figure 3. a) Molecular structure of Hexa-peri-hexabenzocoronene, b) The Honeycomb model of Hexa-peri-hexabenzocoronene.

Example 1. Suppose that HBC is the honeycomb structure of Hexa-peri-hexabenzocoronene is shown in Figure 3(b). With geometric transformations, the configuration of Figure 3(b) can be changed as shown in Figure 4. According to the honeycomb structure studied in Figure 2, one can consider the structure HBC containing the graph G that has the honeycomb structure with 4 cells in rows and 3 cells in columns and two paths with labels $\{a, b, c\}$ and $\{d, e, f\}$ added according to Figure 4.

First, we obtain the dominating set and the domination number of graph G. Let D be the dominating set of the structure HBC. According to Figure 4, if D_i is the dominating set of subgraph G_i for $i = 1, 2$, then, using Theorem 1, we have

$$D_i = \{1, 5, 9, 12, 16\}.$$

To dominate the vertices $\{a, b, c, d, e, f\}$, the set of vertices $\{b, e\}$ must belong to D. Therefore, the dominating set of HCB is as $D_1 \cup D_2 \cup \{b, e\}$. Thus, by Theorem 1, we obtain

$$\gamma(HBC) = \gamma(G) + 2 = (4 + 1)\lceil\frac{3}{2}\rceil + 2 = 12.$$

For obtaining the total dominating set and the total domination number of the structure HBC, if TD_i is the total dominating set of subgraph G_i for $i = 1, 2$, then, using Theorem 2, we have

$$TD_1 = \{2, 3, 6, 7, 8, 11, 13, 15, 17\},$$

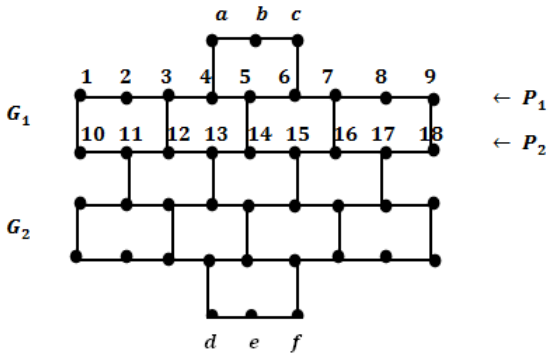


Figure 4. The structure HBC obtained from Figure 3(b)

and

$$TD_2 = \{2, 4, 6, 7, 11, 12, 15, 16, 17\}.$$

On the other hand, with selecting the vertices set $\{a, b, d, e\}$ on paths P_1 and P_2 the total dominating set of the structure HBC is as follows:

$$TD_1 \cup TD_2 \cup \{a, b, d, e\}.$$

Therefore, by Theorem 2, we obtain

$$\gamma_t(HBC) = \gamma_t(G) + 4 = 2(4 + 1) + 4(3 - 1) + 4 = 22.$$

Similar to determining the dominating set and using Theorem 3, the independent dominating set of the structure HBC is as $ID_1 \cup ID_2 \cup \{b, e\}$, where ID_i for $i = 1, 2$ are as follows:

$$ID_1 = ID_2 = \{1, 5, 9, 12, 16\}.$$

Therefore, the independent domination number of HBC is $\gamma_i(G) + 2 = 12$.

We obtain the connected dominating set of G using Theorem 4 as follows:

$$CD_1 = \{2, 3, 4, \ldots, 8, 11, 12, 16, 17\},$$

and

$$CD_2 = \{2, 3, 4, 7, 8, 11, 12, 13, 16, 17\}.$$

Therefore, one can select the connected dominating set of the structure of HBC as follows:

$$CD_1 \cup CD_2 \cup \{a, d, e\}.$$

Thus, the connected domination number of HBC is as $\gamma_c(HBC) = \gamma_c(G) + 3 = 24$.

Finally, we obtain the doubly connected dominating set of the structure HBC by Theorem 6. In this way, the subsets CCD_i of graph G are as follows:

$$CCD_1 = \{1, 2, 5, 6, \ldots, 11, 14, 15, \ldots, 18\},$$

and

$$CCD_2 = \{1, 2, 3, 8, 9, 10, \ldots, 18\}.$$

Therefore, for the doubly connected dominating set of the structure HBC, we get

$$CCD_1 \cup CCD_2 \cup \{b, c, d, e, f\}.$$

Thus, the doubly connected HBC is $\gamma_{cc}(HBC) = \gamma(G) + 5 = 27 - 4\lceil\frac{3}{2}\rceil + 9 + 5 = 32$.

For studying the domination parameters on other molecular structures that are similar to the honeycomb structure studied in this paper, these parameters can be easily computed.

Honeycomb structures are lightweight and flexible cellular structures having enormous applications in the aerospace industry, high-speed automobiles, computers and other electronics equipment bodies. A major challenge in this field is to understand the topological properties of honeycomb structures. In the next example, we study the kind of honeycomb structure as a graded honeycomb structure (GHS) (see Figure 5(a)). We consider the structure studied in [27] that has 6 rows and 15 cells in each row.

We investigate the domination parameters on the structure GHS as one of the topological properties in the honeycomb structure. For this

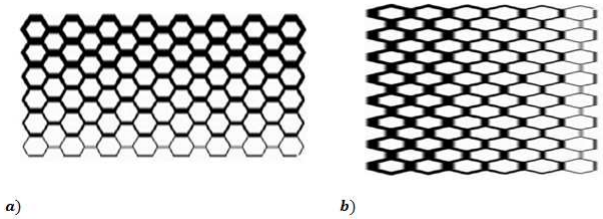


Figure 5. a) The modified graded honeycomb structure (GHS), b) Rotate Figure 5(a) 90 degrees counterclockwise

purpose, we consider the honeycomb structure GHS shown in Figure 5(b), which can be obtained by rotating 90 degrees counterclockwise of Figure 5(a). Based on the change, the structure GHS has $n = 6$ cells in rows and $k = 15$ cells in columns. Therefore, we compute easily the domination parameters of GHS using the theorems in Section 2.

Example 2. Suppose that GHS is the honeycomb structure of graded honeycomb structure is shown in Figure 5(a) with 6 rows and 15 cells in each row. With considering Figure 5(b) and using Theorem 1, the domination number of the structure GHS is obtained as follows:

$$\gamma(GHS) = (6+1)\lceil\frac{15}{2}\rceil = 56.$$

Using Theorem 2, the total domination number of GHS is as follows:

$$\gamma_t(GHS) = 2(6+1) + 6(15-1) = 98.$$

For other domination parameters, using Theorem 3, Theorem 4 and Theorem 6 we get

$$\gamma_i = (6+1)\lceil\frac{15}{2}\rceil = 56.$$

Also, the connected domination number of GHS is equal to

$$\gamma_c(GHS) = 2\lceil\frac{15}{2}\rceil(12-3) + 1 = 145,$$

and the doubly connected domination number of GHS is

$$\gamma_{cc}(GHS) = 15(12+1) - 4\lceil\frac{15}{2}\rceil + 9 = 172.$$

References

[1] L. Wahl, S. Maas, D. Waldmann, A. Zurbes, and P. Freres, "Shear stresses in honeycomb sandwich plates: Analytical solution, finite element method and experimental verification," *Journal of Sandwich Structures and Materials*, vol. 14, pp. 449–468, 2012.

[2] Q. Zhang *et al.*, "Bioinspired engineering of honeycomb structure – Using nature to inspire human innovation," *Progress in Materials Science*, vol. 74, pp. 332–400, 2015.

[3] P. Manuel, B. Rajan, I. Rajasingh, and M.C. Monica, "On minimum metric dimension of honeycomb networks," *Journal of Discrete Algorithms*, vol. 6, pp. 20–27, 2008.

[4] I. Stojmenovic, "Honeycomb networks: Topological properties and communication algorithms," *IEEE Transactions on Parallel and Distributed Systems*, vol. 8, pp. 1036–1042, 1997.

[5] P. Holub, M. Miller, H. Perez-Roses, and J. Ryan, "Degree Diameter Problem on Honeycomb Networks," *Discrete Appl. Math*, vol. 179, pp. 139–151, 2014.

[6] P. Manuel, B. Rajan, J. Rajasingh, and C. Monica,"On minimum metric dimension of honeycomb networks," *Journal of Discrete Algorithms*, vol. 6, pp. 20–27, 2008.

[7] B. Rajan, I. Rajasingh, and F. Xavier, "Harmonious colouring of honeycomb networks," *Journal of Computer Science and mathematical Sciences*, vol. 6, pp. 882–887, 2011.

[8] I. Rajasingh, A. Muthumalai, R. Bharati, and A. S. Shanthi, "Packing in honeycomb networks," *Journal of Mathematical Chemistry*, vol. 50, no. 5, pp. 1200–1209, 2012.

[9] I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks," *IEEE Trans. Parallel Distributed Systems*, no. 1, pp. 14–25, 2002.

[10] Amritha Sampath, C. Tripti, and Sabu M. Thampi, "An ACO algorithm for effective cluster head selection," *J Adv Inf Technol*, vol. 2. no. 1, pp. 50–56, 2011.

[11] A. Vazquez, "Optimal drug combinations and minimal hitting sets," *BMC Systems Biology*, vol. 3, no. 81, 2009. doi: 10.1186/1752-0509-3-81

[12] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, *Fundamentals of Domination in Graphs*, New York: Marcel Dekker Inc., 1998.

[13] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, *Domination in Graphs - Advanced Topics*, New York: Marcel Dekker Inc., 1998.

[14] S. A. Abed and H. M. Rais, "Hybrid bat algorithm for minimum dominating set problem," *Journal of Intelligent and Fuzzy Systems*, vol. 33, no. 4, pp. 2329-2339, 2017.

[15] M. Garey, D. S. Johnson,*Computers and Intractability: A Guide to the Theory of NP-completeness*, 1st ed., W. H. Freeman, 1979, 340 p. ISBN-10: 0716710455. ISBN-13: 978-0716710455.

[16] S. Guha and S. Khuller, "Approximation algorithms for connected dominating set," *Algorithmica*, vol. 20, pp. 374–387, 1998.

[17] M. Rai, S. Verma, and S.Tapaswi, "A Power aware minimum connected dominating set for wireless sensor networks," *J. Netw*, vol. 4, pp. 511–519, 2009.

[18] R. Gandhi and S. Parthasarathy, "Distributed algorithms for connected domination in wireless networks," *J. Parallel Distrib. Comput*, vol. 67, pp. 848–862, 2007.

[19] S. Bermudo, R. A. Higuitab, and J. Rada, "Domination in hexagonal chains," *Applied Mathematics and Computation*, vol. 369, 124817 (2020).

[20] D. A. Mojdeh, M. Habibi, and L. Badakhshian, "Total and connected domination in chemical graphs," *Italian Journal of Pure and Applied Mathematics*, vol. 39, pp. 393–401, 2018.

[21] A. Klobucar and A. Klobucar, "Total and Double Total Domination Number on Hexagonal Grid," *Mathematics*, vol. 7, 1110 (2019).

[22] E. Sampathkumar and H. Walikar, "The connected domination number of a graph," *Journal of Mathematical and Physical Sciences*, vol. 13, pp. 607–613, 1979.

[23] J. Cyman, M. Lemanska, and J. Raczek, "On the doubly connected domination number of a graph," *Central European Journal of Mathematics*, vol. 4, pp. 34–45, 2006.

[24] Z. Wang, Y. Zhang, and J. Liu, "Comparison between five typical reinforced honeycomb structures," in *5th International Conference on Advanced Engineering Materials and Technology (AEMT 2015)*.

[25] A. Kaveh, *Optimal Analysis of Structures by Concepts of Symmetry and Regularity*, Wien-New York: Springer, 2013.

[26] S. Helga, B. Purushothaman, D. J. Jones, A. B. Holmes, and W. W. H. Wong, "Hexa-peri-hexabenzocoronene in organic electronics," *Pure and Applied Chemistry*, vol. 84, pp. 1047–1067, 2012.

[27] S. A. Galehdari and H. Khodarahmi, "Design and analysis of a graded honeycomb shock absorber for a helicopter seat during a crash condition," *International Journal of Crashworthiness*, vol. 21, no. 3, pp. 231–241, 2016.

Fateme Movahedi, Kok Keong Choong,
Mohammad Hadi Akhbari

Received November 04, 2021
Accepted November 22, 2021

Fateme Movahedi
Department of Mathematics, Faculty of Sciences,
Golestan University, Gorgan, Iran
E–mail: f.movahedi@gu.ac.ir

Kok Keong Choong
School of Civil Engineering, Universiti Sains Malaysia,
Nibong Tebal, Penang, Malaysia
E–mail: cekkc@usm.my

Mohammad Hadi Akhbari
Department of Mathematics, Estahban Branch,
Islamic Azad University, Estahban, Iran
School of Civil Engineering, Universiti Sains Malaysia,
Nibong Tebal, Penang, Malaysia
E–mail: mhakhbari20@gmail.com

Split logarithm problem and a candidate for a post-quantum signature scheme

A.A. Moldovyan, N.A. Moldovyan

Abstract

A new form of the hidden discrete logarithm problem, called split logarithm problem, is introduced as primitive of practical post-quantum digital signature schemes, which is characterized in using two non-permutable elements A and B of a finite non-commutative associative algebra, which are used to compute generators $Q = AB$ and $G = BQ$ of two finite cyclic groups of prime order q. The public key is calculated as a triple of vectors (Y, Z, T): $Y = Q^x$, $Z = G^w$, and $T = Q^a B^{-1} G^b$, where x, w, a, and b are random integers. Security of the signature scheme is defined by the computational difficulty of finding the pair of integers (x, w), although, using a quantum computer, one can easily find the ratio $x/w \bmod q$.

Keywords: finite associative algebra, non-commutative algebra, finite cyclic group, discrete logarithm problem, hidden logarithm problem, public key, digital signature, post-quantum cryptosystem.

MSC 2010: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50

1 Introduction

In the current field of development of post-quantum cryptographic algorithms and protocols [1], considerable attention of the world cryptographic community is paid to the development of two-key cryptographic schemes on algebras [2], [3], on Boolean functions [4], [5], and on linear codes [6], [7]. To develop a public-key cryptoscheme that is resistant to an attack including computations on a hypothetic quantum computer

©2022 by CSJM; A.A. Moldovyan, N.A. Moldovyan
doi:10.56415/csjm.v30.14

(quantum attack), one should use the computationally complex problems different from the factoring problem and the discrete logarithm problem (DLP), since each of them can be solved in polynomial time on a quantum computer [8]–[10].

The hidden discrete logarithm problem (HDLP) defined in the finite non-commutative associative algebras (FNAAs) is very attractive as a primitive of practical post-quantum digital signature (DS) schemes [11]–[13]. Several different forms of the HDLP and design criteria of the HDLP-bases DS schemes are considered in the papers [14], [15].

For a more complete understanding of the potential of the HDLP as a post-quantum cryptographic primitive, it is interesting to expand the set of forms of defining the HDLP. This article offers a new form called split logarithm problem (SLP). Next Section 2 considers the notions of DLP and HDLP and used notations. Section 3 introduces a novel form of the HDLP and a SLP-based signature scheme. Section 4 presents discussion and Section 5 concludes the paper.

2 Preliminaries

2.1 Use of the exponentiation as a base operation of public-key cryptoschemes

In the finite associative algebraic structures, the exponentiation can be performed sufficiently fastly and allows one to define a computationally complex problem, called DLP, well suitable for designing public-key cryptoschemes of different types (public key-agreement protocols, public encryption algarithms, signature schemes) and commutative encryption algorithms. The DLP is defined in a finite cyclic group as problem of finding an integer value x satisfying the equality

$$Y' = Q^x, \tag{1}$$

where Q is the group generator; Y' and Q are known elements of the group. Formula (1) is used to generate a public key in different DLP-based cryptoschemes. To set a required security of cryptoschemes, i. e., fairly high difficulty of the DLP, the group order should be prime and

have large size (256 to 2048 bits and more, depending on the type of the used cyclic group). In the known DLP-based DS schemes, the values Q and Y' are used as parameters of signature verification equations, i. e., usually they are public parameters of cryptoschemes. Since the Shor quantum algorithm [8] allows one to find effectively the logarithm value in any explicitly given cyclic group, the DLP-based cryptoschemes are not resistant to quantum attacks.

The idea of the HDLP consists in using the exponentiation as the base operation introducing the main contribution to the security of the public-key cryptoschemes and masking the parameters of the base cyclic group (the group in which the exponentiation operation is performed to calculate a public key). Thus, in the HDLP-based cryptoschemes the base cyclic group is hidden. Obviously, the HDLP must be set in some finite algebraic support, which includes a sufficiently large number of different cyclic groups, forming an environment in which some fixed cyclic group can be securely hidden. In addition, masking operations must have some special properties that ensure the correct operation of the cryptoscheme.

Different types of the FNAAs of different even dimensions have been proposed for their use as algebraic support of the HDLP-based cryptoschemes [3], [16]. The non-commutativity of the multiplication operation is a principal property of the FNAAs for defining the HDLP, which allows one to set the masking operations possessing the required properties, one of which is mutual commutativity with the exponentiation operation. The latter is provided when using the automorphism-map φ_A and homomorphism-map ψ_H operations for masking the base cyclic group. Masking operations are secret, therefore they should be dependent on selection of some random values.

The φ_A operation, parameterized by an invertible algebra element A, is defined in an FNAA containing a two-sided global unit E by the formula

$$\varphi_A(X) = AXA^{-1}, \tag{2}$$

where X takes on all values in the algebra. The $\psi_{L,H}$ operation, parameterized by a left-sided unit L and a locally invertible element H, can be defined in an FNAA containing a large set of left-sided global

units [17] by the formula

$$\psi_{L,H}(X) = HXH', \tag{3}$$

where X takes on all values in the algebra and the algebra element H' is such that $HH' = H'H = L$. It is easy to see that each of the masking operations set by the formulas (2) and (3) is mutually commutative with the exponentiation operation: $\varphi_A\left(X^k\right) = \left(\varphi_A(X)\right)^k$ and $\psi_{L,H}\left(X^k\right) = \left(\psi_{L,H}(X)\right)^k$. Some other types of masking operations are considered in [11], [13].

When using masking operation set by the formula (2), in the DS scheme [12] on a 4-dimensional FNAA the public key is formed as follows:

1. Select at random a non-invertible vector B generating a cyclic group of prime order q having fairly large size and a random non-negative integer $x < q$.

2. Select at random an invertible element G such that $GB \neq BG$ and calculate the first element Y of the public key: $Y = GB^xG^{-1}$.

3. Select at random an invertible element H such that $HB \neq BH$ and $GH \neq HG$ and calculate the second element Z of the public key: $Z = HBH^{-1}$.

4. Calculate the third element T of the public key: $T = GRH^{-1}$, where R is an invertible vector representing a local right-sided unit of the vector B (formulas describing sets of local right-sided anf left-sided units are presented in [12]).

The elements of the public key (Y, Z, T) are contained in three different cyclic groups and no element of the hidden group generated by the non-invertible vector B is known. To generate a signature only one secret parameter (the integer x) can be used, although many other secret values are used to calculate the public key. Therefore, one can define this form of the HDLP as finding the private key x that is discrete logarithm in a hidden group.

A certain disadvantage of the signature scheme [12] is the use of a hidden group generated by a non-invertible element of the FNAA used as algebraic support. However, in the signature scheme [12] based on this form of the HDLP, the said flaw seems to be unavoidable. In

section 3 of this paper, a new form of the HDLP, called SLP, is proposed, the application of which makes it possible to avoid using the signature scheme parameters that are non-invertible elements of the algebra. This possibility is due to the used new masking mechanism that consists in performing two exponentiation operations in two different cyclic groups of the same prime order, which are set by some two fixed secret elements of the FNAA.

2.2 The used algebraic support

To be used as algebraic support of the HDLP form proposed in the present paper, an FNAA should i) contain a two-sided global unit and ii) contain a sufficiently large set of cyclic groups of prime order q having a sufficiently large size (256 bits or more). Many FNAAs satisfying the first requirement are described in the literature, for example, see [11], [12], [16]. To satisfy the second criterion, an FNAA can be set over the finite ground field $GF(p)$, the characteristic of which has the structure $p = eq+1$, where q is a 256-bit prime; e is a small even number (usually $e = 2$).

As the used algebraic support, we have chosen the 4-dimensional FNAA defined over $GF(p)$ and described in [18]. We also use notations of [18]: $\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2$, and $\mathbf{e}_3$ are formal basis vectors; $a_0, a_1, a_2, a_3 \in GF(p)$ are coordinates of a vector $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + a_3\mathbf{e}_3$ that can be alternatively written as $A = (a_0, a_1, a_2, a_3)$. The vector multiplication operation of two vectors A and $B = b_0\mathbf{e}_0 + b_1\mathbf{e}_1 + b_2\mathbf{e}_2 + b_3\mathbf{e}_3$ is defined by the following formula

$$AB = \left(\sum_{i=0}^{3} a_i\mathbf{e}_i\right)\left(\sum_{j=0}^{3} b_j\mathbf{e}_j\right) = \sum_{j=0}^{3}\sum_{i=0}^{3} a_i b_j\left(\mathbf{e}_i\mathbf{e}_j\right),$$

where the product $\mathbf{e}_i\mathbf{e}_j$ for all possible pairs of the integers i and j is to be replaced by some single-component vector $\lambda\mathbf{e}_k$ indicated in the cell at intersection of the ith row and the jth column of so called basis vector multiplication table (BVMT) shown as Table 1, where $\lambda \neq 0$. The value $\lambda \neq 1$ is called structural constant.

Our choice is due to the fact that the vector multiplication operation in this algebra is given by a sparse BVMT, which reduces the compu-

Table 1. Setting the multiplication operation in the used FNAA [18].

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	0	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	0	$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	0

tational complexity of multiplication and exponentiation operations by two times. The latter leads to a twofold increase in the performance of the developed signature scheme. In addition, the structure of the said FNAA is investigated in detail, and results of [18] show the algebra includes only three types of commutative subalgebras having the same order equal to p^2:

i) multiplicative group of which is generated by a minimum generator system containing two vectors of order $p-1$, the group order being equal to $(p-1)^2$; number of such subalgebras is equal to $p(p+1)/2$;

ii) multiplicative group of which is cyclic and has order $p(p-1)$; number of these subalgebras is equal to $p+1$;

iii) multiplicative group of which is cyclic and has order p^2-1; number of these subalgebras is equal to $p(p-1)/2$.

In this paper, we consider the case of defining the FNAA over the finite ground field $GF(p)$ characteristic of which has the structure $p = 2q+1$, where q is a 512-bit prime, and of using the cyclic groups of the order q that is a divisor of $p-1$, which are contained in the set of the commutative subalgebras of the first type. The vector $E = (1,1,0,0)$ is the global two-sided unit of the algebra. A vector G satisfying the condition $g_0g_1 \neq \lambda g_2g_3$ is invertible.

3 The split logarithm problem and a SLP-based signature scheme

3.1 Proposed form of the HDLP

Proposition 1. Suppose invertible vectors A and B are not permutable, and the vector $Q = AB$ has prime order equal to q. Then the vector $G = BA$ also has order equal to q.

Proof. By the condition, $Q^q = E \Rightarrow A(BA)^{q-1}B = E \Rightarrow A(BA)^{q-1} = B^{-1} \Rightarrow (BA)^{q-1} = A^{-1}B^{-1} = (BA)^{-1} \Rightarrow G^{q-1} = G^{-1}$ and $G^q = E$. Proposition 1 is proven. □

Proposition 2. Suppose invertible vectors A and B are not permutable; $Q = AB$ and $G = BA$. Then the equality $Q^k = AG^{k-1}B$ holds true.

Proof. $Q^k = (AB)^k = A(BA)^{k-1}B \Rightarrow AG^{k-1}B$. Proposition 2 is proven. □

Using the algorithm [18] for the generation of a group having 2-dimensional cyclicity, one can easily generate at random a vector Q' of order $p-1$, which is not a scalar vector, and compute the vector $Q = Q'^2$ having order equal to q. Then, fixing a vector A that is not permutable with Q, one can compute the vectors $B = A^{-1}Q$ and $G = BA$. The proposed new form of the HDLP follows from the next procedure for generating a public key that will be used in the signature scheme described in the Subsection 3.2 of the article:

1. Generate two random vectors A and B such that both of the vectors $Q = AB$ and $G = BA \neq Q$ have the same order q and the vector G is not a scalar vector.

2. Select at random non-negative integer $x < q$ and a primitive element α (modulo p). Then compute the first public key element $Y = (AB)^x\alpha = Q^x\alpha$.

3. Select at random non-negative integer $w < q$ and compute the second public-key element $Z = (BA)^w = G^w$.

4. Generate two random integers $a < q$ and $b < q$ and calculate the third signature element $T = Q^aB^{-1}G^b$.

Note that each of the vectors Q and G together with a scalar vector

$N = (n, n, 0, 0)$, where $n \in GF(p)$ is an element of order q, compose a minimum generator system of a 2-dimensional cyclicity group (contained in a commutative subalgebra of the first type).

The calculated public key (Y, Z, T) is intended for use in a DS scheme in which the known parameters are the parameters for setting the algebraic support and the public key elements, i. e., the vectors Y, Z, and T. The values x and w represent logarithms of the values Y and Z contained in two different cyclic groups (in the case, when the basis of logarithm is hidden, i. e., unknown). All other values used while calculating the public key are secret. The known value T connects the said cyclic groups. The logarithms x and w are connected via the public-key element T and one can propose a method for generating a signature, when using the values of the ratio $x/w \bmod q$ and α (see alternative signature generation algorithm in the next Subsection 3.2). Therefore, the introduced form of the HDLP can be called split logarithm problem (SLP).

3.2 Candidate for a practical post-quantum DS scheme

To generate a signature to some electronic document M, the owner of public key (Y, Z, T) (a person that had supposedly generated this key) should use some secret parameters, the set of which is called a private key. In the proposed SLP-based signature scheme it is sufficient to use only three secret values, namely, integers x, w, and α. However, in this case, an alternative signature generation procedure is to be applied, in which two exponentiation operations are executed; whereas, when using the private key, including the values A, G, x, w, α, and d $(d = a + b \bmod q)$, the following signature generation procedure, including only two exponentiation operations, outputs a genuine signature.

Algorithm for generating a signature.

1. Generate at random an integer $k < q$ and an integer $\rho < p$. Then calculate the vector $R = AG^k\rho$.

2. Compute the first 512-bit signature element e from the document M to which the vector R is concatenated: $e = f_H(M, R)$, where f_H is a pre-agreed collision-resistant 512-bit hash-function.

3. Compute the second 512-bit signature element s:

$$s = \frac{k - d - ex + 1}{x + we} \bmod q.$$

4. Compute the third 512-bit signature element σ: $\sigma = \rho\alpha^{-(e+s)}$.

On the average, computation of a 1024-bit signature (e, s, σ) requires performing one exponentiation operation in the FNAA (6144 multiplications modulo p) which makes a major contribution to the computational complexity of the signature generation procedure and one exponentiation operation in $GF(p)$ (768 multiplications modulo p). The verification of the signature (e, s, σ) to the document M is performed using the public key (Y, Z, T) and the following algorithm.

Signature verification algorithm.

1. Using the public key, compute the vector R':

$$R' = Y^{e+s}TZ^{se}\sigma.$$

2. Compute the hash-function value $e' = f_H(M, R')$.

3. If $e' = e$, then the signature is accepted as a genuine one. Otherwise, the signature is rejected.

The computational complexity of the signature verification procedure is roughly equal to two exponentiation operations in the FNAA used as algebraic support and one exponentiation operation in $GF(p)$ (totally, ≈ 13056 multiplications modulo p).

Correctness proof of the developed SLP-based signature scheme implies demonstrating that the correctly computed signature (e, s) passes the verification procedure as a genuine one. Due to Propositions 1 and 2, we have the following:

$$\begin{aligned} R' = Y^{e+s}TZ^{se}\sigma &= Q^{xe+xs}\alpha^{e+s}Q^aB^{-1}G^bG^{wse}\rho\alpha^{-(e+s)} = \\ &= Q^{xe+xs+a}B^{-1}G^{wse+b} = AG^{xe+xs+a-1}BB^{-1}G^{wse+b} = \\ &= AG^{s(x+we)+xe+d-1}\rho = A \circ G^k\rho = R \;\Rightarrow\; R' = R \;\Rightarrow\; e' = e. \end{aligned}$$

Alternative signature generation algorithm.

1. Generate at random integers t $(0 < t < q)$, u $(0 < u < q)$, and ρ $(0 < \rho < p)$. Then calculate the vector $R = Y^t T Z^u \rho$ (note: $R = AG^k \rho$, where $k = tx - 1 + a + b + wu \bmod q$).

2. Compute the value $e = f_H(M, R)$.

3. Compute the value s:

$$s = \frac{(t-e)x + wu}{(x + we)} \bmod q = \frac{(t-e)xw^{-1} + u}{(xw^{-1} + e)} \bmod q. \qquad (4)$$

4. Compute the third signature element σ: $\sigma = \rho\alpha^{-(e+s)} \bmod p$

4 Discussion

One of the features of the proposed signature scheme is the use of the scalar multiplication operation when calculating the first element Y of the public key and vectors R (in the signature generation algorithm) and R' (in the signature verification algorithm). Without introducing scalar multiplication operations, the signature scheme is somewhat simplified, but the rationale for using multiplications by scalars is that they make it computationally feasible to construct a periodic function with a period length that depends on the values of x and w. Consider a simplified version of the proposed signature scheme with the signature (e, s), when calculation of the first public-key element and the said vectors is executed by the following formulas: $Y_0 = (AB)^x = Q^x$, $R = AG^k$, and $R' = Y^{e+s} T Z^{se}$.

Proposition 3. The private key elements A and G satisfy the inequality $AG \neq GA$, i. e. they are not permutable.

Proof. Assume the opposite: $AG = GA$. Taking into account that $G = BA$, we have: $ABA = BA^2 \Rightarrow ABAA^{-1} = BA^2A^{-1} \Rightarrow AB = BA$. The latter equality contradicts the fact that in the proposed signature scheme, the vectors A and B are not permutable. Proposition 3 is proven. □

Proposition 4. For integer variable $k = 0, 1, \ldots q-1$, the function $F(k) = AG^k$, where A and G are elements of the private key of the introduced signature scheme, takes on values in q different cyclic groups.

Proof. Assume the opposite: for some two integes k and t, satisfying the conditions $0 \le k < q$ and $0 \le t < k$, the vectors $F(k)$ and $F(t)$ are contained in the same cyclic group Γ of some order ω. The latter means that for some two integers i and j (suppose for the sake of certainty that $i > j$) we have $F(k) = V^i$ and $F(t) = V^j$, where V is a generator of the cyclic group Γ, i. e., $AG^k = V^i$ and $AG^t = V^j$. Therefore, $AG^k = V^i = V^j V^{i-j} = AG^t V^{i-j} \Rightarrow G^{k-t} = V^{i-j}$. Since $k - t$ and q are mutually prime numbers, one can write $G = V^{\frac{i-j}{k-t}} = V^z$, where z is an integer number.

Thus, $AG^k = V^i \Rightarrow AV^{kz} = V^i \Rightarrow AV^{kz-i \bmod \omega} = E \Rightarrow A = V^{-(kz-i) \bmod \omega}$. The latter equality means that $A \in \Gamma$; therefore, A and V are permutable: $AV = VA \Rightarrow AG^k = AV^{zk} = V^{zk}A = G^k A$, i. e. $AG^k = G^k A$. Taking into account that $G = \left(G^k\right)^{z'}$, where the integer $z' = k^{-1} \bmod q$, one gets: $A\left(G^k\right) = \left(G^k\right)A \Rightarrow AG = GA$, i. e. the vectors A and G are permutable. However, this contradics Proposition 3. The resulting contradiction proves Proposition 4. $\square$

According to the public parameters of the simplified signature scheme, you can directly set a periodic function containing a period with a length that depends on the values of x and w, namely, the function $F_0(i, j) = Y_0^i T Z^j$ in two integer variables i and j. Proposition 4 shows the values of this function are distributed evenly across q different cyclic groups (note: $F_0(i, j) = AG^{i+j}$).

However, one can specify a periodic function, the use of which makes it possible to calculate the ratio of secret values x and w on a hypothetic quantum computer. Indeed, it is easy to show: $Z^* = TZT^{-1} = Q^w$ and the periodic function $F_0(i, j) = Y_0^i Z^{*j}$ in two integer variables i and j contains a period with the length $(-1, xw^{-1})$:

$$F_0(i-1, j+xw^{-1}) = Y_0^{i-1} Z^{*j+xw^{-1}} = Q^{x(i-1)} Q^{w(j-xw^{-1})} =$$
$$= Q^{xi} Q^x Q^{wj} Q^{-x} = Y_0^i Z^{*j} = F_0(i, j).$$

This function takes on the values in an explicitly specified cyclic group (that is generated by the vector Z^*). Therefore, using the Shor quantum algorithm, one can easily find the period length $(-1, xw^{-1})$ and, using the value of the ratio $\frac{x}{w}$, compute signatures, using the alternative signature generation algorithm.

Using an additional scalar multiplication, when computing the $Y = Q^x\alpha$ element of the public key, constructon of the periodic functions taking on the values in a fixed cyclic group and containing a period depending on the value x or/and w becomes computationally infeasible. Indeed, it is easy to see that the vectors Y and Z^* compose a minimum generator system of a commutative 2-dimensional cyclicity group of order q^2 (since the vectors Y_0 and Z^* are elements of the same cyclic group of order q). Therefore, the function $F(i,j) = Y^i Z^{*j}$ takes on all values in the said group and has a period with the length (q,q). Thus, the criterion of post-quantum resistance [14] is satisfied in the proposed SDL-based signature scheme. This explains why the proposed signature scheme uses vectors Q and G belonging to commutative subalgebras of the first type.

The reductionist security-proof method [19] that was applied to the Schnorr DLP-based signature scheme [20] can also be applied to the developed SLP-based DS scheme. Like in the Schnorr DS scheme, in the developed one, during the signature generation process the base exponentiation operation G^k is performed before calculating the first signature element $e = f_H(M,R)$, where $R = AG^k$.

In the model [19] of reductionist security-proof, it is assumed a signature forger is able to calculate the second signature element s equally well for two different hash functions f_H and f'_H (it is supposed that the hash function f_H is collision-resistant and free of properties that can be used to forge a signature [21]). Using the same input data, the forger executes two computer programs, each of which uses the same value of k, but different hash functions. The forger obtains two different signatures (e,s) and (e',s') for fixed value k and different values e and e'. Thus, the forger gets two linear equations with the unknown value of k and the unknown value of the discrete logarithm x. In the Schnorr signature scheme [20], the discrete logarithm represents one integer x and the second signature element $s = k + ex \bmod q$, therefore, the forger, using the obtained two equations, can calculate the private key x.

In the case of the proposed SLP-based DS scheme, the second signature element can be calculated by the formula (4) with three unknowns $x/w \bmod q$, t, and u, where the ratio x/w represents the split logarithm.

Therefore, the security-proof method [19] is to be extended to the case of forger's computing three different signatures (e_1, s_1, σ_1), (e_2, s_2, σ_2), and (e_3, s_3, σ_3), when using three different hash functions and fixed values of t, u, and ρ (the latter fixes the vector R in the alternative signature generation algorithm). As a result, the forger composes a system of three linear equations with three unknowns: $x/w \bmod q$, t, and u. Then, solving this system, the forger gets the values of every of the indicated unknowns. The unknown value of α is computed as follows:

$$\alpha = \left(\frac{\sigma_1}{\sigma_2}\right)^{(e_2+s_2-e_1-s_1)^{-1} \bmod q}.$$

Thus, an assumption of the existence of an algorithm for breaking the proposed signature scheme leads to the conclusion that there is an effective algorithm for calculating the values of $x/w \bmod q$ and α. This means that the analysis of the security of the proposed signature scheme is reduced to the analysis of the computational complexity of solving the SLP. The latter is the task of independent research.

A rough comparison of the proposed DS scheme with some known candidates for post-quantum signature schemes is presented in Table 2 (in the case of setting the used FNAAs over $GF(p)$ with 512-bit prime p) which demonstrates the introduced SLP-based DS scheme has advantages in the size of parameters and peformance (lower execution time; *estimated in multiplications modulo p), which are significant from a practical point of view.

5 Conclusion

A new form of the HDLP, called SLP, has been proposed as a primitive for developing post-quantum cryptoschemes. A comparison of the developed SLP-based DS scheme with other candidates for post-quantum signature algorithms shows the former is more attractive from a practical point of view due to its smaller size of public key and signature. However, more detailed security analysis is to be performed as independent research work. Developing new forms of the SLP and combining the current version of the SLP with a known form of the HDLP in

Table 2. A rough comparison of some DS schemes.

Signature scheme	signature size, bytes	public-key size, bytes	sign. gener. time*	sign. verific. time*
[14]	256	1536	$\approx 37,000$	$\approx 49,000$
[15]	320	2316	$\approx 83,000$	$\approx 110,600$
[11]	256	1536	$\approx 61,400$	$\approx 49,200$
[12]	128	768	$\approx 12,300$	$\approx 24,600$
Falcon [22]	1280	1793	–	–
Dilithium [23]	2701	1472	–	–
Proposed	128	768	$\approx 6,000$	$\approx 12,300$

framework a single signature scheme also represent interest for further research.

Acknowledgement. *This work was supported by the budget theme No. FFZF-2022-007.*

References

[1] *Post-Quantum Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019*, (Lecture Notes in Computer Science, vol. 11505), 2019.

[2] A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, and A. A. Nechaev, "Cryptographic Algorithms on Groups and Algebras," *Journal of Mathematical Sciences*, vol. 223, no. 5, pp. 629–641, 2017.

[3] N. A. Moldovyan and A. A. Moldovyan, "Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem," *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software*, vol. 12, no. 1, pp. 66–81, 2019. DOI: 10.14529/mmp190106.

[4] G. P. Agibalov and I. A. Pankratova, "Asymmetric cryptosystems on Boolean functions," *Prikl. Diskr. Mat.*, no. 40, pp. 23–33, 2018. DOI: 10.17223/20710410/40/3.

[5] G. P. Agibalov, "ElGamal cryptosystems on Boolean functions," *Prikl. Diskr. Mat.*, no. 42, pp. 57–65, 2018. DOI: 10.17223/20710410/42/4.

[6] Q. Alamelou, O. Blazy, S. Cauchie, and Ph. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, pp. 469–493, 2017.

[7] Y. V. Kosolapov and O. Y. Turchenko, "On the construction of a semantically secure modification of the McEliece cryptosystem," *Prikl. Diskr. Mat.*, no. 45, pp. 33–43, 2019. DOI: 10.17223/20710410/45/4.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer," *SIAM Journal of Computing*, vol. 26, pp. 1484–1509, 1997.

[9] A. Ekert and R. Jozsa, "Quantum computation and Shorś factoring algorithm," *Rev. Mod. Phys.*, vol. 68, p. 733, 1996.

[10] R. Jozsa, "Quantum algorithms and the fourier transform," *Proc. Roy. Soc. London Ser A*, vol. 454, pp. 323-337, 1998.

[11] N.A. Moldovyan and A.A. Moldovyan, "Candidate for practical post-quantum signature scheme," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 16, no. 4, pp. 455–461, 2020. https://doi.org/10.21638/11701/spbu10.2020.410

[12] A.A. Moldovyan and N.A. Moldovyan, "Post-quantum signature algorithms based on the hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 26, no. 3(78), pp. 301–313, 2018.

[13] D.N. Moldovyan, "New Form of the Hidden Logarithm Problem and Its Algebraic Support," *Bulletin of Academy of Sciences of Moldova. Mathematics*, no. 2(93), pp.3–10, 2020.

[14] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "Digital signature scheme with doubled verification equation," *Computer Science Journal of Moldova*, vol. 28, no. 1(82), pp. 80–103, 2020.

[15] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "An enhanced version of the hidden discrete logarithm problem and its algebraic support," *Quasigroups and Related Systems*, vol. 28, no. 2, pp. 269–284, 2020.

[16] N. A. Moldovyan, "Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263–270, 2020.

[17] D. N. Moldovyan, "Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem," *Computer Science Journal of Moldova*, vol. 27, no. 1(79), pp. 56–72, 2019.

[18] D. N. Moldovyan, "A practical digital signature scheme based on the hidden logarithm problem," *Computer Science Journal of Moldova*, vol. 29, no. 2(86), pp. 206–226, 2021.

[19] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.

[20] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, pp. 161–174, 1991.

[21] N. Koblitz and A. J. Menezes, "Another Look at "Provable Security"," *Journal of Cryptology*, vol. 20, pp. 3–38, 2007.

[22] "Fast-Fourier lattice-based compact signatures over NTRU," https://falcon-sign.info/

[23] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A Lattice-Based DigitalSignature Scheme," https://eprint.iacr.org/2017/633.pdf (see also https://pq-crystals.org/dilithium/index.shtml).

A. A. Moldovyan, N. A. Moldovyan

Received January 21, 2021
Accepted February 21, 2022

St. Petersburg Federal Research Center of
the Russian Academy of Sciences (SPC RAS)
14 Liniya, 39, St.Petersburg, 199178
Russia
E–mail: nmold@mail.ru

A Comparative study on classification performance of Emphysema with transfer learning methods in deep convolutional neural networks

Selçuk Yazar

Abstract

Today Emphysema, which takes place among the top five diseases, is encountered in the western world in terms of rehabilitation and healthcare costs. Diagnosis of this type of respiratory tract disease with the help of computers is gradually increasing its importance. In this study, we aimed to classify it with the transfer learning method by using single labeled emphysema diagnosed data which is obtained from three large data sets. We classified the images that are obtained from ChestX-ray14, CheXpert, and PadChest databases by 95% of Area Under the Curve (AUC) with the fully connected layer model and DenseNet-121 pre-trained neural network and 90% of Area Under the Curve (AUC) with Xception pre-trained neural network. We evaluated this proposed deep learning-based model as an effective and practical diagnostic tool for emphysema alone, using x-ray data. Notably, transfer learning is a very functional approach in terms of differentiation between normal and patient in similar diseases that have just emerged in the pandemic period that we live in.

Keywords: Deep Learning, Transfer Learning, Convolutional Neural Networks, Medical Imaging, Emphysema Diagnosis.

MSC 2010: 68T10, 92C50, 92B20.

©2022 by CSJM; S. Yazar
doi:10.56415/csjm.v30.15

1 Introduction

Emphysema is defined as the main type of lung condition known as a chronic obstructive pulmonary disease (COPD). The most important etiological factor of the disease is a smoking habit, the effects of which are expressed in various ways. In addition to smoking, other inhaled pollutants such as cadmium chloride, nitrogen oxides, and phosphagen are also identified as the main factors that cause this disease. Especially with the increase of smoking in the community, the increase in emphysema cases is important. In low- and middle-income countries, 90% of deaths occur due to emphysema and related COPD [1]. It is accepted that there are more than 200 million patients worldwide. However, the incidence of the disease is higher in industrialized settlements, where air pollution rates are high. Generally, the mild form of emphysema is quite common. The prevalence of individuals close to the age of 70 is quite high and it is more common in men. Although the pathogenesis (origin and development) of the disease is a complex process, there are two fundamental mechanisms. The first is structural fragility due to elastolysis (lack of elastic tissue) in the lungs, and the second is the loss of airway support.

As a result of the abnormal activity of proteolytic (protein-dissolving) enzymes, this disease causes irreversible destruction of alveolar walls in the lungs and expansion of distal air spaces. If it is defined in general, it can be called as airway obstruction. The symptoms that cause such morphological changes in the lungs mentioned here are difficult to detect with conventional radiographic imaging techniques [2] because the decrease in tissue density caused by emphysema can occur in very small sizes. Today, chest X-ray images are frequently used for this type of diagnosis for respiratory tract diseases. However, chest X-rays are known to be devoid of sensitivity in mild to moderate emphysema. The screening for emphysema detection is very often done today with the method called spirometric lung function test, which is based on numerically evaluating how much a patient breathes and how much of this breath can be extracted within a certain period of time. Of course, the cooperation of the patient is very important in this type of method. On the other hand, this screening method cannot be used

to locate emphysematous changes in the lung. Determining the regional distribution of emphysema is very important for making clinical decisions if the patient will undergo lung volume reduction surgery.

New imaging techniques are helpful in the face of the difficulty of detecting the disease from these aspects. There are very good improvements in the detection of this disease with high-resolution computed tomography (HRCT) [3]. However, its use is limited to the high radiation dose applied to the patient. Some studies on this subject recommend using Magnetic Resonance Imaging (MRI) techniques as supplementary/complementary to Computed Tomography applications for the detection of emphysema. However, MRI applications are relatively expensive, difficult to access, and prone to breathing artifacts, preventing it from becoming a routine approach used in the diagnosis of this disease. It is an important issue to directly evaluate the microstructural damage in the alveolar network caused by emphysema, to see the course of the disease and the treatment results. However, in this case, histopathological interventional biopsy methods are still applied as a valid approach. Methods such as biopsy always pose a risk to the patient and burden time and cost.

Clinical X-ray imaging, which is frequently used in the medical world today, can be defined as the application of image creation depending on the X-Ray absorption properties of tissues and materials in the human body. Medical imaging is based on a physical phenomenon called photoelectric absorption. X-ray absorption is a variable that depends on approximately the fourth time the atomic number value of the atoms of a material or medium, denoted as Z [4]. Thanks to this feature, skin, bones, etc., it is ensured that the required image contrast is obtained between materials of different densities. The second feature that is effective in medical imaging is the depth of penetration. The depth of penetration of X-Rays corresponds approximately to the third times the photon energy for a given material. By adjusting the value of the photon energy, it is possible to obtain the appropriate penetration depth depending on the material being worked on.

Diagnosis and severity of pulmonary emphysema on chest radiographs are difficult, especially in the early stages of the disease. Conventional chest radiographs can visualize indirect signs of increased

lung volume seen in emphysema, such as flattened diaphragm, widely spaced ribs, increased chest diameter, and increased retrosternal air space in lateral view. In conclusion, chest radiograms have been shown to be reasonably accurate for advanced emphysema, but to be moderately sensitive in mild to moderate emphysema with inter-observer variability [5-8].

In general, there are many publications in which different imaging techniques are used in the diagnosis of thoracic diseases. The approaches used in these publications can be divided into two groups. These two groups can be listed as chest x-ray and computed tomography. Artificial intelligence methodologies were frequently used in both of these groups. Especially in recent years, many methods have been tried using chest x-ray images. Convolutional Neural Networks (CNN) methods have yielded very successful results in this group. Some of the methods performed are as follows: classification of disease [9], determination of lungs by segmentation [9], and determination of pathological nodule and mass by localization [10]. Along with these methods, the methods of standardizing chest x-ray images and editing them with different approaches were also applied. These studies [11] in the ChestX-ray14 database are in the form of using the images in the database for the training of the artificial neural network. One of the most common problems encountered in the studies here is that the images in this archive are not uniform. There are many artifacts in the pictures, such as noise from medical equipment. Another problem is that pictures cannot be used in full resolution in artificial neural network training. Reducing the resolution brings the risk that small size and vital lesions will not be noticed. Successful researches have also been made to solve these two problems. In addition, the DenseNet [12, 13] neural network, which has been produced to solve these problems, has limited performance, although it also gives successful results. A remarkable study is the merging of two different artificial neural networks separated by the segmentation method using multiple tagging [14].

CheXpert, the database of Stanford University, is used in successful studies, especially in the diagnosis of pneumonia and lung cancer [15]. The best results obtained from this data set are listed on a website on a date basis and made available to researchers. Similarly, the PadChest

is a preferred database by researchers for use in multi-label disease diagnosis. Here, there is a study on the production of labels for medical images with natural language processing methods [16]. Although the last two databases are not as popular as ChestX-ray14, they are often preferred in research.

In this study, we aimed to correctly identify emphysema patients by transfer learning method and analyzing chest X-ray data with the help of deep learning approaches. The first novelty here is the use of three large databases around the world. Secondly, Xception and DenseNet-121 pre-trained artificial neural networks were used to classify patients diagnosed with emphysema only in these databases.

2 Material and Methods

2.1 Data Sources

There are many respiratory system disorders such as bronchitis, pneumonia, asthma, pleural effusion (accumulation of water in the lung membrane), especially emphysema. Today, there are three data sets available to researchers worldwide for the detection of these diseases with machine learning methods. These data sets provide highly detailed X-ray images and diagnostic details for scientists who want to do research on this subject.

One of the data sets used in this study is the ChestX-ray14 [11] database provided by the National Institute of Health (NIH) in the United States. In this database, there are 112,120 anterior view chest x-rays of approximately 30,805 patients. The diagnostic information in this dataset includes 14 respiratory system diseases (thorax). The main ones can be listed as Pneumonia, Pneumothorax, Emphysema, Fibrosis, and Pleural Thickening. Another data set we used is the PadChest database of Alicante University in Spain [17]. In this database, there are 160,000 images of 67,000 patients. This set contains multi-labeled information on 19 different diagnoses. Images in the PadChest database were taken from six different angles. Finally, another data set we use is the CheXpert database provided by Stanford University [18]. In this database, there are 224,316 chest x-ray images of 65,240

patients. This set also includes diagnostic information for 14 different thoracic diseases such as ChestX-ray14.

The common feature of these databases is that there are cases in which the diagnosis of emphysema disease is alone, as well as data that have been diagnosed with other diseases. The diagnosis of emphysema, which is labeled multiple, is more than just a single labeled diagnosis. In this study, we used only data diagnosed with emphysema disease alone. In total, the number of data diagnosed with emphysema alone is 1,594. However, these images have been increased to 3,190 with augmentation to be used in the artificial neural network. The data sets and the information about the data numbers that we used are shown in Table 1.

Table 1. The number of images and sources used during the study, which are only diagnosed with emphysema (with augmentation)

Dataset name	Diagnosis type count	Single labeled emphysema diagnosis
ChestX-ray14	14	1,046
CheXpert	14	1,018
PadChest	19	1,126
Total Emphysema		3,190
		Normal Labeled Images
Total Normal	-	2,617
General		5,807

Similarly, no disease was diagnosed in the same number in total from the same data sets, and we included the data in our study. The number of data we use for healthy patients is 2,617. As a result, we employed a total of 5,807 data to be used in the input layer of the model in the study. We used a distribution of 80% training, 15% verification, and 5% testing in our dataset. The rates of data distribution are shown in Figure 1.

Deep learning algorithms, especially convolutional neural networks (CNN), are a highly reliable approach that is often used to learn pre-

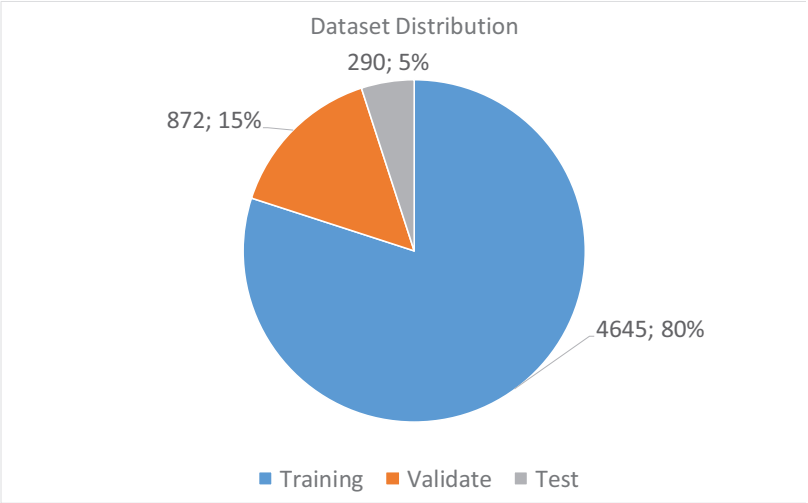


Figure 1. Distribution of data used in training our artificial neural network

dictive properties using visual data directly [19]. There are many deep CNN models for object detection and classification such as ResNet [20], InceptionV3 [21], and Xception [22], which are frequently used today. In 2015, the ResNet model succeeded in winning the ImageNet Large-Scale Visual Recognition Challenge with an error rate of %3.6 [23]. The Xception model we preferred in this study was derived from the Inception V3 model in 2016. Both models use the ImageNet dataset. CNN's are a frequently preferred method for classifying medical images, and new studies are constantly being conducted on them today. The basis of the performance of ESA is the provision of a large amount of data. However, if the data set to be studied is of small size, the success in training the artificial neural network decreases. At this stage, the transfer learning method offers a powerful option to avoid memorization during the learning of limited data [24].

The training of the artificial neural network in transfer learning is carried out in two stages. In the first step, using the fundamental weights of a pre-trained artificial neural network, fine-tuning is done

for the data set being studied. Then, using the weights of the neural network that are obtained here is retrained with the layers of the new neural network added to the pre-trained neural network. Here the main reason for the approach is the relatively small size of the researched data set. However, the smallness of the data set in this study is to be able to classify the disease from the data of patients diagnosed with emphysema alone.

2.2 Preprocessing of X-ray Data

Many different methods and algorithms have been proposed for the classification of thoracic diseases by artificial intelligence. In this study, we aimed to classify images without any procedure, especially in images obtained and diagnosed with emphysema. However, when we examined the data sets, we realized that the images in the data set were not in the same standard. In addition to the image quality, the total number of images diagnosed with the disease remained below 2.000. Here, we used visual augmentation methods that are frequently preferred in CNN models. This augmentation process is used to prevent overfitting of the model. For this purpose, 28% magnification, 10% width shift range, 20% rotation operations were applied to the images. The pictures obtained from the data sets were reduced to 210 x 210 x 1 dimensions for use in the Xception and DenseNet-121 model. Moreover, the Contrast Limited Adaptive Histogram Equalization (CLAHE) filter, which is known to give good results in medical images, was applied to all images here. In this method, histogram equalization is performed by looking at the values of a central pixel in a local window [25]. The effect of the CLAHE filter in a sample image can be seen in Figure 2. This filter has greatly improved some images, especially in the PadChest dataset.

2.3 Implementation of Model

In this study, we first based on the Xception pre-trained neural network for use in emphysema classification. Xception [22], is based on the assumption that the correlation between the input channels can be completely separated from the spatial correlation. Xception in particular extends the initial architecture by replacing the standard convolution

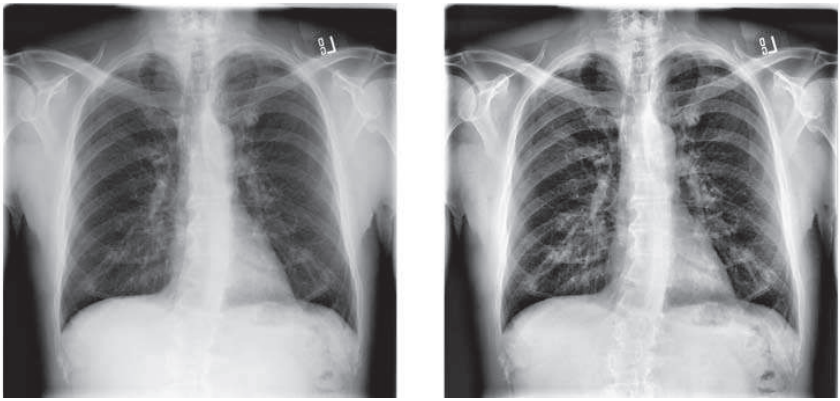


Figure 2. A sample x-ray image with a CLAHE filter applied

with a deeply independent convolution. Thus, this network is defined as a linear stack of deep collapsible layers with permanent connections. In visual classification studies, transfer learning or fine-tuning according to the size of the data set to be applied is a novel approach. The behavior pattern to be determined in the CNN training here is developed by considering the size and similarities of the data sets. If there is a small data set, learning transfer can be done depending on the fact that it is obtained from different and same sources, and fine-tuning can be done in case of having large data. However, these are not binding when it comes to research. Transfer learning (TL) is a method that transfers the pre-trained artificial neural network from the source area to the target area in order for the CNN model to have a better image recognition ability. In the studies conducted, it was revealed that the TL-CNN models have better generalizations, and their qualities in extracting strong image features, apart from the training data, were shown [26, 27]. However, since the TL needs the transfer of pre-trained weights and parameters, the TL-CNN models have a different working process and different efficiencies in training and testing compared to their prototypes.

The transfer learning method used in CNN is applied in two ways. The first of these is the method called a bottleneck. This method is

based on training by replacing fully connected layers in the last part of a pre-trained artificial neural network (eg. ImageNet) with newly determined CNN layers. The important approach here is to obtain input weights by freezing the convolution layers of the first neural network while determining the bottleneck properties. Later, these frozen layers are activated and the values obtained in the previous step are transferred to the newly formed network. Another method is called the "Heating" method. In this method, the fully connected layers that we created in the model are determined randomly according to the Xception network which we have added. In the existing Xception neural network, there is a risk of losing the properties of the pre-trained neural network if the weights of these new fully bonded layers are not prevented from back-propagation. Normally, when an artificial neural network is being trained, the backpropagation process is stopped after fully connected layers. In this way, the artificial neural network enables feature extraction in the inversion layers. Unlike the bottleneck method, some parts of the network created in the fine-tuning process are excluded from the training, especially the entrance parts, and only fully connected layers are trained. Then the entire network is retrained with fully connected layers. The TL and fine-tuning approach that we have applied in this study is shown in Figure 3.

In this study, we have prepared the weights obtained with the Flatten layer after the Xception / DenseNet network, which is taken as the basis for the classification process, to be sent to two fully connected layers. The network model we have created has two Dense, that is, fully connected layers. Since we are using the last fully connected layer 2 class in our model, there are two inputs. For the transfer of learning, we first trained for frozen layers in the artificial neural network for 25 epochs. At this stage, the total number of parameters of the network is 21 million for Xception based model. Approximately 20 million of these parameters are non-trainable. In the next step, the neural network was trained for 100 epochs, together with the network structure designed by us. In this second stage, the total of untrained parameters is 8 million. We used the root mean square error method for optimization. In addition, we set the learning rate as 0.00001 at the beginning and the decreased value as 0.004.

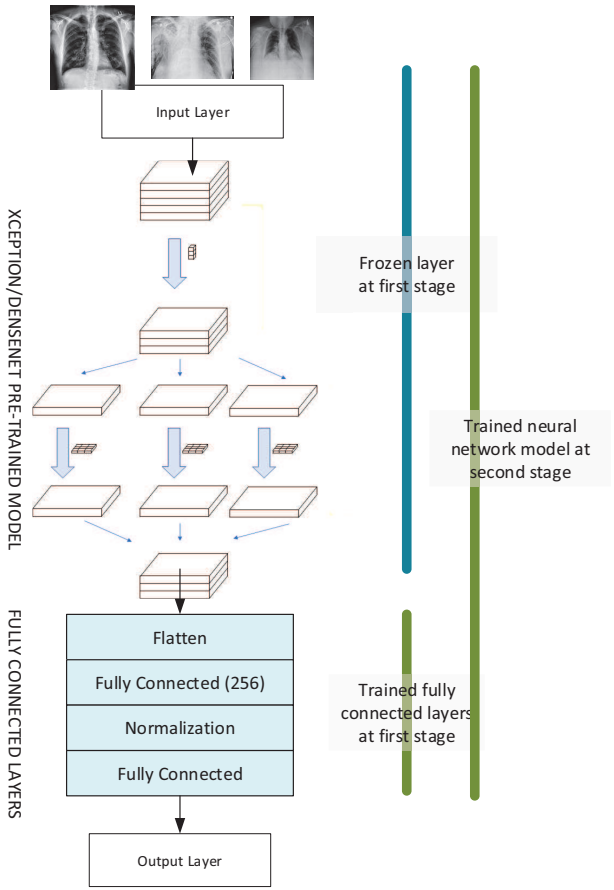


Figure 3. Artificial neural network model and training method with transfer learning

3 Results and Discussions

In this study, we tried to classify a total of 5,807 images obtained from three separate databases with only emphysema diagnosis. We developed the application and used it for classification using Python and Keras. We conducted our experiments using the Google Colab platform by serving our data on Google Drive. The training of the fully connected layers we used in our Xception Model took 1 hour 25 minutes and the training of the entire network took 5 hours 24 minutes. During our experiments, we tried to get the best results by testing various hyper-parameters. For the Xception pre-trained artificial neural network we could reach in this study, the highest Validate Accuracy was 86.44% and the highest AUC score was 90%. This value can be considered good when compared with many studies.

For the Xception model we created, the verification precision (val_acc) of the fully connected layers we first created resulted in 74.61%. Later, as a result of the training we conducted for the entire artificial neural network, we determined the accuracy of the verification as 86.44%. There are many respiratory system disease classification studies using the data sets we used in this study. As mentioned earlier in these studies, successful results have been obtained by using multiple classification methods and different deep learning models. As can be seen in these studies, the DenseNet pre-trained network gives very good results in the classification of x-ray images. However, there is limited work done with the Xception network in the literature. This paper yielded the best results compared to a small number of studies conducted using three different data sets and classifying only the diagnosis of emphysema. The values and comparisons of the results we obtained are shown in Table 2.

A distinctive feature in these studies is that auxiliary algorithms are also used in visual classification. For instance, in I. Allaouzi[28], firstly, the lung region in the data in the data set was separated by segmentation and the diagnosis classification was made accordingly. Studies with low AUC scores are directed towards the classification of X-ray data and special algorithms are not preferred. This raises the need for these data to be prepared according to certain standards be-

Table 2. Comparisons of previous studies and the proposed Xception based model

Author(s)	Dataset(s)	Label	AUC Score	F1 Score	Model
I.Allaouzi[28]	ChestX-ray14, CheX-pert	Multi	0.94-0.926	0.56-0.63	DenseNet
X. Wang et al.[11]	ChestX-ray14	Multi	0.833	0.95	ResNet
L. Yao et al.[29]	ChestX-ray14	Multi	0.842	Not Shared	DenseNet
S. Gündel et al.[12]	ChestX-ray14	Multi	0.895	Not Shared	DenseNet 121
L. Han et al.[14]	ChestX-ray14	Multi	0.921	Not Shared	DenseNet 121
C. Mao et al. [30]	ChestX-ray14	Multi	0.8823	Not Shared	DenseNet 169
H. Wang [31]	ChestX-ray14	Multi	0.8222	Not Shared	ChestNet
E. Çallı et al. [32]	ChestX-ray14	Single	0.854	Not Shared	ResNet5.0
P. Rajkupar et al.[33]	ChestX-ray14	Multi	0.9371	Not Shared	DenseNet 121
S. Rakshit et al.[34]	ChestX-ray14	Multi	0.9351	Not Shared	ResNet18
S. M. Sushavan et al.[35]	ChestX-ray14	Multi	0.52	Not Shared	Xception
Our Proposal	ChestX-ray14, CheX-pert, Padchest	Single	0.82	0.75	Xception

fore being subjected to excessive pre-processing. Apart from Table 3, Y. Wang et al. [36], in their study, stated the AUC score as 99.06% with ChesNet2, which they developed using DICOM visuals. However, in the mentioned study, no value was shared especially regarding emphysema.

In our experiments, we created a model in the same way by using the similar TL method and DenseNet weights. In our DenseNet-121 application, we preferred not to change the hyper-parameters and optimization functions we created earlier. In our training, we obtained with this model the highest values as 93.75% accuracy and 95% AUC scores among the results of the studies that are shown in Table 3. Among these studies, the studies in which we reordered DenseNet users and their results are shown in Table 3.

The ROC graph of the model training we did with the DenseNet121 network during the study is shown in Figure 4.

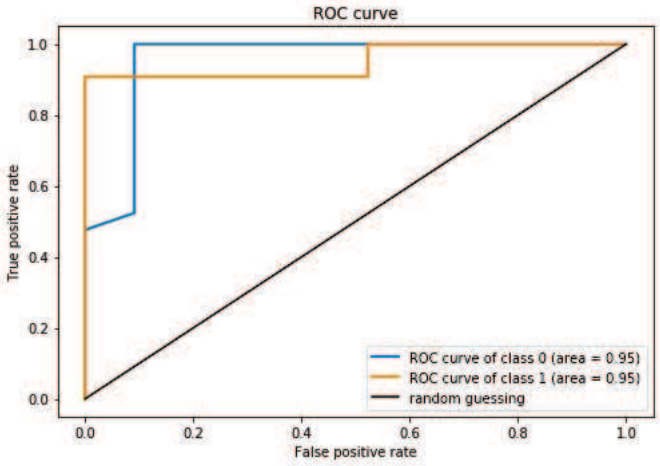


Figure 4. ROC curve of classification success of DenseNet-121 artificial neural network

The high AUC score we obtained in the experiments and evaluated the classification that we made was successful. Undoubtedly, we think that we will make great progress in the diagnosis of this disease with

Table 3. Comparison of previous studies and proposed model using DenseNet-121

Author(s)	Dataset(s)	Label	AUC Score	F1 Score	Model
I.Allaouzi[28]	ChestX-ray14, CheX-pert	Multi	0.94-0.926	0.56-0.63	DenseNet
L. Yao et al.[29]	ChestX-ray14	Multi	0.842	Not Shared	DenseNet
S. Gündel et al.[12]	ChestX-ray14	Multi	0.895	Not Shared	DenseNet 121
L. Han et al.[14]	ChestX-ray14	Multi	0.921	Not Shared	DenseNet 121
C. Mao et al. [30]	ChestX-ray14	Multi	0.8823	Not Shared	DenseNet 169
Our Proposal	ChestX-ray14, CheX-pert, Padchest	Single	0.95	0.94	DenseNet 121

new approaches to be produced by adding more original data obtained from different databases. In general, only one data set was used in studies in the literature. In addition, the diagnosis of emphysema disease is classified together with diagnoses seen with more than one thoracic disease. The records of patients diagnosed with emphysema alone, which we used in this study, are relatively few compared to patients diagnosed with more than one respiratory disease. In diagnoses related to the disease, it is difficult to determine it apart from other disease diagnoses, but it gives high results when it is classified together with very specific diseases such as pneumonia, requiring further research on whether it is a health classification. Especially, it may be a preferred method to

detect respiratory system diseases that cause such micro damages by computed tomography rather than x-ray. It is clear that medical image classification studies will not be used in decision-making instead of the experts. However, it has a guiding feature in order to assist medical doctors in the diagnosis of these diseases.

In this study, we have shown that the transfer learning method is a successful method in such medical classification applications if the data sets are different and the number of data is low. Especially with the Covid-19 pandemic, we are experiencing today, it has once again revealed the importance of artificial intelligence applications in diagnosing with medical images. Since lung lesions caused by Covid-19 also cause damage to alveoli like emphysema, their detection is promising with the methodologies mentioned in this study. Especially in this disease, even if the blood tests are negative, the definitive diagnosis of this disease can be made with computer-aided tomography images. Image recognition models that will distinguish Covid-19 infection from standard pneumonia show high success. In addition, new methods are being developed to better show the situation in human tissues in standard X-ray images. With the advancing technology, artificial intelligence models that can classify these images as successfully as computed tomography images will be developed.

4 Additional Info

Data sets of the developed models and models of the study can be accessed at github.com/MachineLearningLessons/DenseNetEmphysema.

References

[1] P. J. Friedman, "Imaging studies in emphysema," *Proceedings of the American Thoracic Society*, vol. 5, no. 4, pp. 494–500, 2008.

[2] M. Morgan, "Detection and quantification of pulmonary emphysema by computed tomography: a window of opportunity," *Thorax*, vol. 47, no. 12, p. 1001, 1992.

[3] J. E. Takasugi and J. D. Godwin, "Radiology of chronic obstructive pulmonary disease," *Radiologic Clinics of North America*, vol. 36, no. 1, pp. 29–55, 1998.

[4] J. Als-Nielsen and D. McMorrow, *Elements of modern X-ray physics*, John Wiley & Sons, 2011. Print ISBN: 9780470973950. Online ISBN: 9781119998365. DOI: 10.1002/9781119998365.

[5] M. Miniati *et al.*, "Value of chest radiography in phenotyping chronic obstructive pulmonary disease," *European Respiratory Journal*, vol. 31, no. 3, pp. 509–515, 2008.

[6] N. Muller and H. Coxson, "Chronic obstructive pulmonary disease: imaging the lungs in patients with chronic obstructive pulmonary disease," *Thorax*, vol. 57, no. 11, p. 982, 2002.

[7] W. M. Thurlbeck and G. Simon, "Radiographic appearance of the chest in emphysema," *American Journal of Roentgenology*, vol. 130, no. 3, pp. 429–440, 1978.

[8] G. R. Washko, "Diagnostic imaging in COPD," *Seminars in respiratory and critical care medicine*, vol. 31, no. 3, pp. 276–285, 2010.

[9] A. A. Novikov, D. Lenis, D. Major, J. Hladůvka, M. Wimmer, and K. Bühler, "Fully convolutional architectures for multiclass segmentation in chest radiographs," *IEEE transactions on medical imaging*, vol. 37, no. 8, pp. 1865–1876, 2018.

[10] J. G. Nam *et al.*, "Development and validation of deep learning–based automatic detection algorithm for malignant pulmonary nodules on chest radiographs," *Radiology*, vol. 290, no. 1, pp. 218–228, 2019.

[11] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "ChestX-Ray8: Hospital-Scale Chest X-Ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 3462–3471.

[12] S. Guendel, S. Grbic, B. Georgescu, S. Liu, A. Maier, and D. Comaniciu, "Learning to recognize abnormalities in chest x-rays with location-aware dense networks," in *Iberoamerican Congress on Pattern Recognition*, Springer, 2018, pp. 757–765.

[13] G. Huang, Z. Liu, L. v. d. Maaten, and K. Q. Weinberger, "Densely Connected Convolutional Networks," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 2261–2269.

[14] H. Liu, L. Wang, Y. Nan, F. Jin, Q. Wang, and J. Pu, "SDFN: Segmentation-based deep fusion network for thoracic disease classification in chest X-ray images," *Computerized Medical Imaging and Graphics*, vol. 75, pp. 66-73, 2019/07/01/ 2019

[15] H. H. Pham, T. T. Le, D. Q. Tran, D. T. Ngo, and H. Q. Nguyen, "Interpreting chest X-rays via CNNs that exploit disease dependencies and uncertainty labels," arXiv preprint arXiv:1911.06475, 2019.

[16] T. Olatunji, L. Yao, B. Covington, and A. Upton, "Caveats in Generating Medical Imaging Labels from Radiology Reports with Natural Language Processing," 2019.

[17] A. Bustos, A. Pertusa, J.-M. Salinas, and M. de la Iglesia-Vayá, "Padchest: A large chest x-ray image dataset with multi-label annotated reports," arXiv preprint arXiv:1901.07441, 2019.

[18] J. Irvin *et al.*, "Chexpert: A large chest radiograph dataset with uncertainty labels and expert comparison," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2019, vol. 33, pp. 590-597.

[19] G. Litjens *et al.*, "A survey on deep learning in medical image analysis," *Medical Image Analysis*, vol. 42, pp. 60–88, 2017/12/01/.

[20] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[21] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2818–2826.

[22] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1251–1258.

[23] O. Russakovsky *et al.*, "Imagenet large scale visual recognition challenge," International journal of computer vision, vol. 115, no. 3, pp. 211–252, 2015.

[24] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?," in *Advances in neural information processing systems*, 2014, pp. 3320–3328.

[25] K. Zuiderveld, "Contrast limited adaptive histogram equalization," in *Graphics gems IV*, 1994, pp. 474–485: Academic Press Professional, Inc.

[26] M. J. Hasan and J.-M. Kim, "Bearing Fault Diagnosis under Variable Rotational Speeds Using Stockwell Transform-Based Vibration Imaging and Transfer Learning," *Applied Sciences*, vol. 8, no. 12, Article Number: 2357, 2018.

[27] M. Izadpanahkakhk, S. M. Razavi, M. Taghipour-Gorjikolaie, S. H. Zahiri, and A. Uncini, "Deep Region of Interest and Feature Extraction Models for Palmprint Verification Using Convolutional Neural Networks Transfer Learning," *Applied Sciences*, vol. 8, no. 7, Article Number: 1210, 2018.

[28] I. Allaouzi and M. B. Ahmed, "A Novel Approach for Multi-Label Chest X-Ray Classification of Common Thorax Diseases," *IEEE Access*, vol. 7, pp. 64279–64288, 2019.

[29] L. Yao, J. Prosky, E. Poblenz, B. Covington, and K. Lyman, "Weakly supervised medical diagnosis and localization from multiple resolutions," arXiv preprint arXiv:1803.07703, 2018.

[30] C. Mao, L. Yao, Y. Pan, Y. Luo, and Z. Zeng, "Deep generative classifiers for thoracic disease diagnosis with chest x-ray images," in *2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 2018, pp. 1209–1214: IEEE.

[31] H. Wang and Y. Xia, "Chestnet: A deep neural network for classification of thoracic diseases on chest radiography," arXiv preprint arXiv:1807.03058, 2018.

[32] E. Callı, K. Murphy, E. Sogancioglu, and B. van Ginneken, "FRODO: Free rejection of out-of-distribution samples: application to chest x-ray analysis," arXiv preprint arXiv:1907.01253, 2019.

[33] P. Rajpurkar *et al.*, "Chexnet: Radiologist-level pneumonia detection on chest x-rays with deep learning," arXiv preprint arXiv:1711.05225, 2017.

[34] S. Rakshit, I. Saha, M. Wlasnowolski, U. Maulik, and D. Plewczynski, "Deep Learning for Detection and Localization of Thoracic Diseases Using Chest X-Ray Imagery," in *International Conference on Artificial Intelligence and Soft Computing*, Springer, 2019, pp. 271–282.

[35] S. Mondal, K. Agarwal, and M. Rashid, "Deep Learning Approach for Automatic Classification of X-Ray Images using Convolutional Neural Network," in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, IEEE, 2019, pp. 326–331.

[36] Y. Wang, L. L. Sun, and Q. Jin, "Enhanced Diagnosis of Pneumothorax with an Improved Real-time Augmentation for Imbalanced Chest X-rays Data Based on DCNN," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, pp. 1–1, 2019.

Selçuk YAZAR

Received July 7, 2021
Accepted May 4, 2022

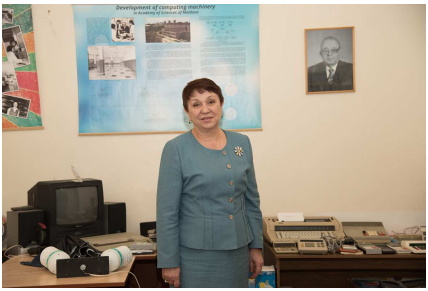
Selçuk Yazar
Kırklareli University Software Engineering Department
Kırklareli / Turkey
Phone:+905327633462
E–mail: selcukyazar@klu.edu.tr

Svetlana Cojocaru – 70th anniversary

Svetlana Cojocaru, born on July 26, 1952, in the village of Butuceni, Râbniţa district, is now a principal scientific researcher of the Vladimir Andrunachievici Institute of Mathematics and Computer Science (IMCS), corresponding member (c.m.), Habilitated doctor in computer science, vice-president of the Academy of Sciences of Moldova.

C.m. Svetlana Cojocaru passed with dignity all the steps of a successful scientific career, being usually characterized with the qualification "first": the first lady Habilitated doctor in IMCS, the first Habilitated doctor in computer science in the Republic of Moldova, the first and, at the moment, the only corresponding member in computer science, etc.

She is known in the community of computer scientists for serious results, materialized in over 240 valuable scientific publications (5 monographs, 7 chapters in monographs, 2 reprinted) at prestigious publishers, editor of 16 collections of articles, materials of national/international conferences and also in useful applications.



Fields of research in which c.m. S. Cojocaru distinguished herself by important achievements are formal grammars and languages, compiler construction, parallel programming, natural language processing, computational algebra, molecular calculations, intelligent interfaces and Information Society Technologies, digitization of cultural heritage, etc.

Even in the first years of research, S. Cojocaru proposed a grammar class with a dispersed context, which allowed both sequential and parallel processing. It was a nice theoretical result that soon became extremely current because it meets the needs of large-scale use of multiprocessor systems for carrying out high-performance calculations. After a while, the formalism of grammars with a dispersed context also found applications in the processing of natural languages. S. Cojocaru

elaborated a formal grammar to describe the inflection process in Romanian, reaching for the first time in the world, the complete solution to the problem of automatic inflection for inflectional languages. Under her leadership, a series of necessary applications were developed: a computational morphological lexicon for the Romanian language with about one million words (displayed for public access on the website www.math.md/elrr), assisted training system for the study of the Romanian language, spelling correction system, etc. These works have an important role in the technologicalization of the Romanian language – a fact that allows a first step towards solving a major problem – the human-computer interaction in natural language.

The results of Hab.Dr. S. Cojocaru have based the research on intelligent interfaces in our country, intending to create a comfortable environment for users from various areas of activity and skill levels. These interfaces offer opportunities to communicate in a subset of natural language in the professional field of user activity. It is worth mentioning that intelligent communication in information systems is an area of high relevance required in European research programs.

C.m. S. Cojocaru was the IMCS leader of a project aimed at developing the Bergman symbolic computing system with an intelligent interface within 5 grants of the Swedish Royal Academy for over 15 years. The results of Hab.Dr. S.Cojocaru in this field are related to the development of the mathematical performances of the system and the elaboration of the interface procedures. The results of the research

in this field ended with the publication of a collection of articles in IOS Press, the Netherlands, as well as a monograph published in Sweden.

In the composition of a group of researchers from IMCS, she studied the problems of building the Information Society in our country and contributed to the development and promotion of information systems, able to solve various problems specific to the Information Society. The report carried out within a UNDP project (2004) was the first approach in our country to the problem of electronic services in public administration (e-government). At the same time, the much-discussed issue of confidentiality and access to information at the community level is based on the public-private model.

C.m. S. Cojocaru participated in studies in the framework of 25 international projects, 7 of them being the team leader. Among the latest studies, some have a pronounced practical character: projects to promote the music culture of Moldova, science management, medical information systems including those for prevention of strokes, non-alcoholic fatty liver, and management of disasters with multiple victims. The results of these studies are mentioned with medals at the exhibitions Infoinvent and "Made in Moldova".

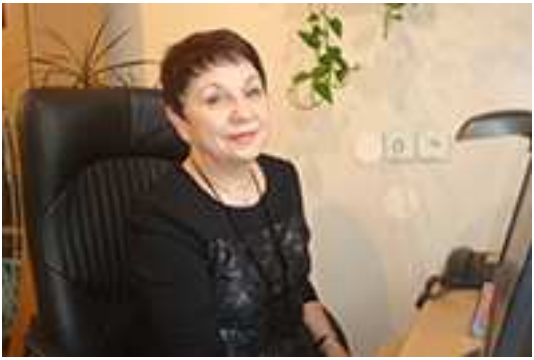
At the beginning of computer science applications, when there were too few knowledgeable persons, S. Cojocaru was the one who initiated the dedication of a group of humanitarian professors from Moldova State University to the "secrets of computer science", giving them

a very inspired course. Also in those times, she published a series of articles in the journal "Femeia Moldovei" in which she acquainted the readers with the first notions of computer science through examples from their practice. This activity of promoting computer science, started many years ago, Hab.Dr. S. Cojocaru successfully continues, expanding the area throughout the world while promoting the image of the country and the science of Moldova – currently being the Vice Editor-in-Chief of the "Computer Science Journal of Moldova". She is a member of the editorial boards of many scientific journals in the country and abroad, including those reviewed in Scopus and Clarivate Analytics.

Another important aspect is the didactic activity and the training of doctoral students. Under her leadership, six scientists defended their doctoral dissertations.

C.m. S. Cojocaru, through her activity, contributed substantially to the development of computer science in the Republic of Moldova, to the affirmation of the Institute of Mathematics and Computer Science "Vladimir Andrunachievici" as a center of excellence with international recognition, to the promotion of the image of Moldovan science.

We sincerely wish her further creative success, successful implementation of her ideas, strength, inspiration, and good health!



Happy birthday, dear prof. Svetlana Cojocaru!

CSJM Editorial Board