International Journal of Theoretical Physics, Vol. 37, No. 1, 1998

# Decomposition of D-Sets

**Olga Nánásiová**[1]

Received July 4, 1997

The main result of this paper is the proof of a connection between abelian groups and difference sets. From this fact we can show that any difference set can be organized to a difference poset as a class of equivalence. We give an example of a difference set as a conditional probability space in the sense of Kolmogoroff.

## 1. INTRODUCTION

*Definition 1.1* (Nánásiová, 1995). Let $L$ be a nonempty set and $\ominus$ be a partial binary operation on $L$. Then the set $L$ will be called a *difference set* (DS) if the following conditions hold:

(d1) for any $a \in L$, $a \ominus a \in L$;
(d2) if $a, b, a \ominus b \in L$, then $a \ominus (a \ominus b) \in L$ and, moreover, $a \ominus (a \ominus b) = b$;
(d3) *the transitive law* if $a, b, c, a \ominus b, b, \ominus c \in L$, then $a \ominus c \in L$ and, moreover, $(a \ominus c) \ominus (a \ominus b) = b \ominus c$.

We will denote $a \ominus a = 0_a$.

*Definition 1.2* (Nánásiová, 1995). Let $L$ be a DS. The set $L$ will be called a *group difference set* (GDS) if the following condition is satisfied:

(d4) $a \ominus b \in L$ iff $b \ominus a \in L$.

*Definition 1.3* (Nánásiová, 1995). Let $L$ be a DS. If $0_b \ominus b \in L$, we define $a \oplus b := a \ominus (0_b \ominus b)$ iff $a \ominus b \in L$.

If $L$ is a DS, then the following properties are satisfied (Nánásiová, 1995):

(1) for any $a \in L$, $a \ominus 0_a \in L$ and $a \ominus 0_a = a$;

[1] Katedra Matematiky a Deskriptívnej Geometrie, Stavebná Fakulta STU, 813 63 Bratislava, Slovenská; e-mail address: nanasio@cvt.stuba.sk.



0020-7748/98/0100-013 1$15.00/0 

(2) if $c \ominus a \in L$, then $0_a = 0_c = 0_{c.a}$;

(3) if $c \ominus a = d$, then $c \ominus d = a$;

(4) if $c \ominus b$, $(c \ominus b) \ominus a \in L$, then $c \ominus a$, $(c \ominus a) \ominus b \in L$ and $(c \ominus b) \ominus a = (c \ominus a) \ominus b$.

If $L$ is a *GDS*, then:

(5) for any $a \in L$, $0_a \ominus a \in L$;

(6) for $a, b, \in L$, $a \ominus b \in L$ iff $0_a = 0_b$;

(7) for $a \ominus b \in L$, $a \ominus b = 0_a \ominus (b \ominus a)$;

(8) the set $G(a) = \{b \in L: 0_a = 0_b\}$ is an Abelian group with respect to the operation $\ominus$;

(9) if for any $a, b \in L$, $0_a = 0_b$, then $L$ is an Abelian group with respect to the operation $\ominus$.

*Proposition 1.1* (Nánásiová, 1995). $L$ is a GDS if it can be written as a disjoint union of abelian groups. Conversely every such disjoint union is a GDS.

From the last proposition it follows that if $L$ is a GDS, then $L$ is an Abelian group iff for every $a, b \in L$, $0_a = 0_b$.

*Lemma 1.2.* Let $L$ be a DS. Then the following properties hold:

(1) If $b, a, 0_a \ominus a \in L$, then $0_a = 0_b$ iff $b \ominus a \in L$;

(2) If $0_a \ominus a, a \ominus b, \in L$, then $0_a \ominus b, b \ominus a \in L$.

*Proof.* (1) It is enough to show that $0_a = 0_b$ implies $b \ominus a \in L$. Let $0_a = 0_b$ and $b, a, 0_a \ominus a \in L$. Then $b \ominus 0_a, 0_a \ominus a \in L$, and from (d3) it follows that $b \ominus a \in L$.

(2) If $0_a \ominus a, a \ominus b, \in L$, then (d3), $0_a \ominus b \in L$ and $a \ominus 0_a, 0_a \ominus b \in L$ imply that $b \ominus a \in L$. ■

If $L$ is a DS and for any $a, b \in L$, $0_a = 0_b$, then from the previous lemma we get that $a, 0 \ominus a \in L$ implies that for any $b \in L$, $b \ominus a$ exists in $L$. If $0 \ominus a, a \ominus b \in L$, then $0 \ominus b, b \ominus a \in L$. An example will show that $b \ominus a, a \ominus b, \in L$ does not imply $0 \ominus a, 0 \ominus b \in L$.

## 2. D-POSET AND GROUP

In the following we will assume $L$ is a DS with only one zero. This means that for any $a, b \in L$, $0_a = 0_b$.

*Definition 2.1.* Let $L$ be DS. A subset of $L$, $I(0) = \{b \in L; a \ominus b, b \ominus a \in L\}$, will be called a *zero class.*

*Lemma 2.1.* Let $L$ be a set with the properties (d1), (d2). Then the transitive law (d4) is fulfilled iff the following associative law holds: If $a,$

$b$, $a \ominus b$, $(a \ominus b) \ominus c \in L$, then $a \ominus c$, $(a \ominus c) \ominus b \in L$ and $(a \ominus b) \ominus c = (a \ominus c) \ominus b$.

*Proof.* It is enough to show only that the associative law implies (d4), because the opposite implication is proved in Nanasiova (1995). Let $a \ominus b$, $b \ominus c \in L$. Then $b = a \ominus (a \ominus b)$, hence $b \ominus c = [\mathrm{a} \ominus (a \ominus b)] \ominus c$. This implies that $a \ominus c$, $(a \ominus c) \ominus (a \ominus b) \in L$, and $(a \ominus c) \ominus (a \ominus b) = b \ominus c$. ■

*Lemma 2.2.* Let $L$ be DS. Then the following properties hold:
(1) If $a \ominus b \in I(0)$, then $0 \ominus (a \ominus b) = (b \ominus a)$.
(2) For any $a, b, \in I(0)$, $a \ominus b$ is defined and belongs to $I(0)$.
(3) The zero class $I(0)$ is an Abelian group.
(4) For any $a \ominus L$ and any $b \in I(0)$ the element $a \ominus b$ is defined.
(5) If $a \in L$, $b \in I(0)$, and $b \ominus a$ is defined, then $a \in I(0)$.

*Proof.* (1) Let $a \ominus b \in I(0)$. From the definition of $I(0)$ it follows that $0 \ominus (a \ominus b)$ is defined and moreover.

$$0 \ominus (a \ominus b) = (a \ominus a) \ominus (a \ominus b) = (a \ominus (a \ominus b)) \ominus a = b \ominus a$$

(2) Let $a, b \in I(0)$. Then $a \ominus 0$, $0 \ominus b$ implies $a \ominus b \in L$. On the other hand, $b \ominus 0$, $0 \ominus a$ implies $b \ominus a \in L$. And from (1) we get $a \ominus b \in I(0)$.

(3) Let $a, b \in I(0)$; then we define the operation $a \oplus b := a \ominus (0 \ominus b)$. In the following we show that the set $I(0)$ is an Abelian group with operation $\oplus$.

From (2) it follows that $a \ominus (0 \ominus b)$, $b \ominus (0 \ominus a)$, $(0 \ominus a) \ominus b$, $(0 \ominus b) \ominus a \in I(0)$. And then $((0 \ominus b) \ominus a) \ominus ((0 \ominus a) \ominus b) \in I(0)$ and moreover

$$\begin{aligned}
&((0 \ominus b) \ominus a) \ominus ((0 \ominus a) \ominus b) \\
&\quad = [(0 \ominus b) \ominus ((0 \ominus a) \ominus b)] \ominus a \\
&\quad = [(0 \ominus ((0 \ominus a) \ominus b)) \ominus b] \ominus a = [(b \ominus (0 \ominus a)) \ominus b] \ominus a \\
&\quad = [(b \ominus b) \ominus (0 \ominus a)] \ominus a = [0 \ominus (0 \ominus a)] = a \ominus a = 0
\end{aligned}$$

From this it follows that $(0 \ominus b) \ominus a = (0 \ominus a) \ominus b$. Then $0 \ominus (0 \ominus b) \ominus a) = 0 \ominus ((0 \ominus a) \ominus b)$ and so $b \ominus (0 \ominus a) = a \ominus (0 \ominus b)$. This means $a \oplus b = b \oplus a$.

Let $a, b, c \in I(0)$. Then $(a \oplus b) \oplus c$, $(a \oplus c) \oplus b) \in I(0)$, and $(a \oplus b) \oplus c = (a \ominus (0 \ominus b)) \ominus (0 \ominus c) = (a \ominus (0 \ominus c)) \ominus (0 \ominus b) = (a \oplus c) \oplus b)$.

Let $c, d, a \in I(0)$ and $c \oplus a = d \oplus a$. Then $= c \ominus (0 \ominus a) = d \ominus (0 \ominus a)$. From this we get

$$(0 \ominus a) \ominus c = (0 \ominus a) \ominus d$$

$$d = (0 \ominus a) \ominus ((0 \ominus a) \ominus c) = c$$

For any $a \in I(0)$, $a \oplus (0 \ominus a) = a \ominus (0 \ominus (0 \ominus a)) = a \ominus a = 0$.
This means that $I(0)$ is an Abelian group.

(4) Let $a \in L$ and $b \in I(0)$. Then $a \ominus 0$, $0 \ominus b$ implies $a \ominus b$.
(5) Let $a \in L$, $b \in I(0)$, and $b \ominus a \in L$. Then $0 \ominus b$, $b \ominus a \in L$ implies $0 \ominus a \in L$.

From this it follows that $a \in I(0)$. ■

Let $a \in L$ and $k \in I(0)$. Then $a \oplus_b k := a \ominus (0 \ominus k)$.

*Lemma 2.3.* Let $L$ be a DS. If for $a \in L$ we define $I(a) = \{b \in L;\ b \ominus a \in I(0)\}$. Then the following statements hold.
(1) For any $b, c \in I(a)$, $c \ominus b \in I(0)$.
(2) The element $b \in I(a)$ iff $I(b) = I(a)$.
(3) For any $a \in L$, $I(a) = \{a \ominus k;\ k \in I(0)\}$.
(4) For any $a \in L$, $I(a) = \{a \oplus_L k;\ k \in I(0)\}$.
(5) For any $a \in L$ and for any $p, q \in I(0)$, $a \ominus (p \oplus q) = (a \ominus p) \ominus q$.
(6) Let $b, a \in L$ and $c \in I(0)$; then $a \ominus (b \ominus c)$ is defined and moreover

$$(a \ominus (b \ominus c)) = (a \ominus b) \ominus (0 \ominus c)$$

(7) Let $b \in I(a)$, $c \in I(d)$, and $a \ominus d \in L$. Then

$$b \ominus d \in L$$

and moreover $b \ominus c \in I(a \ominus d)$.

*Proof.* (1) If $b, c, \in I(a)$, then $b \ominus a$, $a \ominus c \in L$. This implies $b \ominus c \in L$. On the other hand $c \ominus a$, $a \ominus b$ implies $c \ominus b \in L$. This means that $c \ominus b \in I(0)$.
(2) Let $b \in I(a)$. Then $a \ominus b \in I(0)$. This implies $a \in I(b)$. Moreover, if $c \in I(a)$, then $c \ominus b \in I(0)$. From this it follows that $I(a) = I(b)$.
(3) Let $b \in I(a)$. Then $a \ominus b \in I(0)$. This means that there is $k \in I(0)$ such that $a \ominus b = k$. Then $a \ominus k = b$. From this $I(a) = \{a \ominus k;\ k \in I(0)\}$.
(4) It follows directly from definition $\oplus_L$ and (3).
(5) Let $a \in L$ and $p, q \in I(0)$. Then $a \ominus (p \oplus q)$, $a \ominus p \in I(a)$. Then $I(a) = I(a \ominus p)$ and so $(a \ominus p) \ominus q \in I(a)$. From this it follows that there is $[(a \ominus p) \ominus q] \ominus [a \ominus (p \oplus q)]$ and moreover

$$
\begin{aligned}
&[(a \ominus p) \ominus q] \ominus [a \ominus (p \oplus q)] \\
&\quad = [(a \ominus p) \ominus [a \ominus (p \oplus q)]] \ominus q \\
&\quad = [(a \ominus [a \ominus (p \oplus q)]) \ominus p] \ominus q \\
&\quad = [(p \oplus q) \ominus p] \ominus q = [(p \ominus (0 \ominus q)) \ominus p] \ominus q \\
&\quad = [(p \ominus p) \ominus (0 \ominus q)] \ominus q = (0 \ominus (0 \ominus q)) \ominus q = \mathrm{q} \ominus q = 0
\end{aligned}
$$

And so $(a \ominus p) \ominus q = a \ominus (p \oplus q)$.

(6) Let $a, b \in L$ and $c \in I(0)$. Then $a \ominus b$, $b \ominus c$ implies $a \ominus c \in L$ and

$$(a \ominus c) \ominus (a \ominus b) = b \ominus c$$

$$(a \ominus c) \ominus (b \ominus c) = a \ominus b$$

$$(a \ominus (b \ominus c)) \ominus c = a \ominus b$$

$$[(a \ominus (b \ominus c)) \ominus c] \ominus (0 \ominus c) = (a \ominus b) \ominus (0 \ominus c)$$

$$(a \ominus (b \ominus c)) \ominus (c \oplus (0 \ominus c)) = (a \ominus b) \ominus (0 \ominus c)$$

$$a \ominus (b \ominus c) = (a \ominus b) \ominus (0 \ominus c)$$

(7) Let $b \in I(a)$, $c \in I(d)$, and $a \ominus d \in L$. Then $b \ominus a$, $a \ominus d$ implies $b \ominus d$ and $b \ominus d$, $d \ominus c$ implies $b \ominus c$.

Because $b \in I(a)$, then there is $k \in I(0)$ such that $b = a \ominus k$. And so

$$b \ominus c = (a \ominus k) \ominus c$$

On the other hand, $c \in I(d)$ and there is $q \in I(0)$ such that $c = d \ominus q$. And so

$$\begin{aligned} b \ominus c &= (a \ominus (d \ominus q)) \ominus k = ((a \ominus d) \ominus (0 \ominus q)) \ominus k \\ &= (a \ominus d) \ominus (k \oplus (0 \ominus q)) \\ &= (a \ominus d) \ominus (k \ominus (0 \ominus (\ominus q))) = (a \ominus d) \ominus (k \ominus q) \end{aligned}$$

This means that $b \ominus c \in I(a \ominus d)$. ■

Let $L$ be a DS and $\mathcal{L} = \{I(a); a \in L\}$. Then $\mathcal{L}$ is the set of the class of equivalence and we can define the operation $\ominus$ on $\mathcal{L}$ in the following way:

$$I(a) \ominus I(b) \quad \text{iff} \quad a \ominus b \text{ is defined}$$

From the previous lemmas $L$ can be organized as a D-poset such that

$$I(a) \leq I(b) \quad \text{iff} \quad I(b) \ominus I(a) \text{ is defined}$$

Now we can formulate the following proposition.

*Proposition 2.4.* Let $L$ be a DS and $\mathcal{L} = \{I(a); a \in L\}$. Then the triple $(\mathcal{L}, \ominus, \leq)$ is a D-poset.

*Proof.* It is enough to show that $\leq$ is a partially ordering.

Let $a \in L$ and $b \in I(0)$. Then $a \ominus b \in L$. Hence $I(0) \leq I(A)$ for any $I(a) \in \mathcal{L}$.

For any $a \in L$, $I(a) = I(0)$. Let $I(a) \leq I(b)$ and $I(b) \leq I(a)$. This means that $a \ominus b$, $b \ominus a \in L$. From this it follows that $I(a) = I(b)$.

Let $I(a) \leq I(b) \leq I(c)$. Then $c \ominus b,\ b \ominus a \in L$. This implies that $c \ominus a$ is defined. Hence $I(a) \leq I(c)$. ■

Let $L$ be a DS. It is clear that the set $\{I(0_a);\ a \in L\}$ is the union of disjoint abelian groups.

*Proposition 2.5.* Let $L$ be a DS. If $D(L) = (L - I(0)) \cup \{0_a;\ a \in L\}$, then a partial relation $\leq$ such that for $a, b \in L$, $a \leq b$ iff $a \ominus b \in D(L)$ is a partial ordering on $L$ and $D(L)$ is a sub-DS.

*Proof.* If $a, b \in L$, and $a \leq b$ and $b \leq a$, then $a \ominus b,\ b \ominus a \in D(L)$ and hence $a \ominus b,\ b \ominus a \in D(L) \cap I(0)$. Therefore $a \ominus b = b \ominus a = 0_a$, and from this we get $a = b$.

It is clear that for any $a \in L$, $a \ominus a = 0_a \in D(L)$.

Let $a \leq b$ and $b \leq c$. From the assumption we have that $c \ominus b,\ b \ominus a \in D(L)$, and hence $c \ominus a \in L$. If $a \ominus c \in L$, then $a \ominus c$ and $c \ominus b \in L$ imply $a \ominus b \in L$. Thus we have $a \ominus b,\ b \ominus a \in L$, hence $a = b$, and therefore $a \leq c$. If $a \ominus c$ does not exist in $L$, then $c \ominus a \in D(L)$ and this implies $a \leq c$.

It is clear that (d1) and (d2) hold in $D(L)$. The property (d3) follows directly from the proof of the transitivity law for the partial ordering $\leq$ on $L$. ■

From the previous results it follows that for any $b \in I(0)$ and $a \in D(L)$ such that $0_a = 0_b$ there holds $b \leq a$.

Let $L$ be a DS. We will say that the zero class of $L$ is *trivial* if $I(0) = \{0_a;\ a \in L\}$. If for any $a, b \in L$, $0_a = 0_b$ and the zero class of $L$ is trivial, then $L$ is the known D-poset (Kôpka and Chovánec, 1994).

If we define the partial operation $\oplus_D$ through

$$a \oplus_D b \text{ exists iff there is } c \in L \text{ such that } c \ominus a = b,\ c \ominus b = a$$

then it is easy to show that for the operation $\oplus_D$, the commutative and the associative law are satisfied, and if $a, b \in I(0)$, then $a \oplus b = a \oplus_D b = a \oplus_L b$. It is clear that for any $a \in L$ and $b \in I(0)$, there exists $a \oplus_D b$ and $a \oplus_D b = a \ominus (0_a \ominus b)$.

## 3. EXAMPLES

It is known that on Boolean algebras, Abelian groups, and orthomodular lattices, a partial operation $\ominus$ can be defined such that these structures are DS. It is not surprising that if $L$ is a Boolean algebra or an orthomodular lattice, then the zero class $I(0)$ is trivial and for $a, b \in L$, $a \ominus b \in L$ iff $a \leq b$. If $L$ is an Abelian group, then $I(0) = L$, because for $a, b \in L$, $a \ominus b = a - b$, where "$-$" is the usual group operation.

*Example 3.1.* Let $G$ be the cyclic Abelian group $\{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10\}$ and for $a, b \in G$, $a \ominus b = a - b$. Then $G$ is a DS.

Let $A_1 = \{0; 1; 7\}$. Then $A_1$ is a DS and $I(0)$ is trivial.

Let $A_2 = \{0; 1; 2; 9\}$. The $A_2$ is not a DS, because $2 \ominus 0; 0 \ominus 0 \in A_2$, but $2 \ominus 9 \notin A_2$.

Let $A_3 = \{0; 1; 2; 3; 4\}$. The set $A_3$ is a DS with the trivial zero class. For any $a, b \in A_3$, $\{a - b, b - a\} \cap A_3 \neq \emptyset$, but, for example, $3 \oplus 2 \notin A_3$.

Let $A_4 = \{0; 1; 2; 5; 6; 7\}$. The set $A_4$ is a DS and $I(0) = \{0; 5\}$, $D(A_4) = \{0; 1; 2; 6; 7\}$. The set $A_4 = \{I(0), I(1), I(2)\}$ is D-poset and $I(1) = I(6) = \{1, 6\}$, $I(2) = I(7) = \{2, 7\}$.

This set provides the answer to the question: "Let $L$ be a DS and $a \ominus b, b \ominus a \in L$. Do the elements $a, b$ belong to $I(0)$?" Our answer is no, because $1; 6 \in A_4$ $1 \ominus 6 \in I(0)$, but $0 \ominus 1; 0 \ominus 6 \notin A_4$.

*Example 3.2.* Let $(\Omega, \mathcal{S}, P)$ be a classical probability space and $P_A$ be a conditional probability measure in the classical sense for a set $A \in \mathcal{S}$, such that $P(A) \neq 0$. Let us denote $\mathcal{P} = \{P_A; A \in \mathcal{S}$ and $P(A) \neq 0\}$ and $\mathcal{P}_0 = \{1 - P_{A^c}; A \in \mathcal{S}$ and $P(A) = 0\}$. Now we define a map $\alpha$ from $\mathcal{S}$ to $\mathcal{P} \cup \mathcal{P}_0$ by the following $\alpha(A) = P_A$ if $P(A) \neq 0$ and $\alpha(A) = 1 - P(A^c)$ if $P(A)$ jy Let $\mathcal{F} = \{\alpha(A); A \in S\}$. Then the double $(\mathcal{F}, \ominus)$ is a DS if the partial operation $\ominus$ is defined as follows:

$$\alpha(A) \ominus \alpha(B) \quad \text{is defined} \quad \text{iff } P(A^c \cap B) = 0$$

and moreover $\alpha(A) \ominus \alpha(B) = \alpha(A \cap B^c)$. If we define on the set $\mathcal{F}$ the partial operation $\oplus$ such that $\alpha(A) \oplus \alpha(B)$ iff $P(A \cap B) = 0$, and moreover $\alpha(A) \oplus \alpha(B) = \alpha(A \cup B)$, then $(\mathcal{F}, \oplus)$ can be organized as an orthoalgebra. The set $I(0) = \{\alpha(A); P(A) = 0$ for $A \in \mathcal{S}\}$ and $I(\alpha(A)) = \{\alpha(B); P(A \triangle B) = 0\}$, where $A \triangle B = (A^c \cap B) \cup (A \cap B^c)$.

## REFERENCES


Kôpka, F., and Chovanec, F. (1994). D-poset, *Mathematica Slovaca,* **44**, 21–34.

Foulis, D. J., and Bennett, M. K. (1994). Effect algebras and unsharp quantum logics, *Foundations of Physics,* **24**, 1325–1346.

Foulis, D. J., and Bennett, M. K. (1995). Suns and products of interval algebras, *International Journal of Theorical Physics,* **33**, 2119–2136.

Nánásiová, O. (1995). D-set and groups, *International Journal of Theoretical Physics,* **34**, 1637–1642.

Kolmogoroff, A. N. (1933). *Grundbegriffe der Wahrscheikchkeilsrechnung*, Springer, Berlin.

Foulis, D. J., Greechie, R. J. and Rüttiman, G. T. (1992). Filters and supports in orthoalgebras, *International Journal of Theoretical Physics,* **31**, 789–802.