Journal of Universal Computer Science, vol. 4, no. 1 (1998), 34-47
submitted: 25/9/97, accepted: 1/11/97, appeared: 28/1/98 © Springer Pub. Co.

On the Algebra of Intervals and Convex Bodies

Svetoslav M. Markov
(Bulgarian Academy of Sciences, Bulgaria
smarkov@iph.bio.acad.bg)

Abstract: We introduce and study abstract algebraic systems generalizing the arithmetic systems of intervals and convex bodies involving Minkowski operations such as quasimodules and quasilinear systems. Embedding theorems are proved and computational rules for algebraic transformations are given.

Key Words: Interval arithmetic, convex bodies, Minkowski operations, commutative semigroups, isomorphic embedding, quasilinear space.
Category: G.1.m, I.1.m

1 Introduction

The solution of mathematical problems involving uncertain (interval-valued, set-valued) parameters stimulates the development of the arithmetic for intervals and convex bodies. Two familiar arithmetic operations for convex bodies A, B, and in particular, for n-dimensional intervals, are the Minkowski operations:

$$A + B = \{c \mid c = a + b,\ a \in A,\ b \in B\}, \tag{1}$$
$$\alpha \cdot B = \{c \mid c = \alpha b,\ b \in B\}, \tag{2}$$

where α is a real number.

This paper is a further step in the algebraic study of Minkowski arithmetic, basically consisting in defining (1)–(2) axiomatically by several of their properties, and logically deducing other properties (see e.g. [Schneider 1993] for such properties). The term "algebra" in the title of this work is used in the sense of "algebraic system". In [Markov 1997] we consider abstract algebraic systems related to compact intervals on the real line. Here we present a generalization of our results for convex bodies via replacing one of the basic assumptions (the trichotomy property) by a weaker assumption (the cancellation law). This change requires a systematic modification of the entire theory presented in [Markov 1997]; therefore the present results are written in a selfcontained manner and can be read independently of the above mentioned work.

Our approach differs from previous contributions in the same area. Axiomatic descriptions of arithmetic systems of intervals and convex bodies have been formulated e.g. in [Kaucher 1977], [Ratschek and Schröder 1977], [Rådström 1952]). Many authors circumvent the difficulties arising from the nonvalidity of the second distributive law by restricting themselves to the relation:

$$(p + q)A = pA + qA, \quad pq \geq 0, \tag{3}$$

and considering only multiplication by nonnegative scalars; this necessarily leads to embedding theorems merely for cones. Our method is different. We first formulate a suitable algebraic framework, enabling us to extend (3) for all p, q,

i. e. to find an expression of $(p+q)A$ by means of the terms pA and qA for the case $pq < 0$. We then formulate a general distributive-like relation valid for all p, q, called "quasidistributive law", and develop the whole theory on such fundament. Useful technical tools are the inner operations for addition and subtraction, which are related to the Hadwiger-Minkowski subtraction introduced in [Hadwiger 1957].

For the sake of simplicity we restrict ourselves deliberately to arithmetic operations and refrain from introducing important order relations such as inclusion; the only exception from this rule is the order relation "$\leq_s$" induced by (1). The merging of the arithmetic operations and the inclusion relations does not present any difficulties and has been already demonstrated in several works, see e.g. [Kaucher 1977]; for the definition of inner operations in interval spaces over vector lattices see e.g. [Markov 1977].

Intervals and convex bodies with Minkowski addition are proper additive abelian (commutative) semigroups $(S, +)$ with cancellation law. This means that for $A, B, C \in S$ the following four relations are satisfied:

1. S is semigroup: $(A+B)+C = A+(B+C)$;
2. S is abelian: $A+B = B+A$;
3. S is proper semigroup (i.e. not a group itself): there exists (at least one) pair A, B, such that $A+X = B$ has no solution for $X \in S$;
4. S satisfies cancellation law (c.l.): $A+C = B+C \Longleftrightarrow A = B$.

Semigroups with properties 1–3 are further reffered as semimodules. Semimodules with c.l. play an important role in the study of convex bodies, especially because they are embedable in groups. Moreover, intervals and convex bodies have neutral element 0, such that $A+0 = A$ for $A \in S$, that is they are monoids. All mentioned properties still do not reflect thoroughly the nature of the convex bodies with respect to Minkowski addition. The core of our work consists in formulating a special additional assumption, requiring that the semimodule S includes a submodule (module = abelian group), and that the opposite operation in the submodule is isomorphically extended over the semimodule. With this assumption the semimodule S becomes a rich algebraic system, very close to a module itself, therefore we call S a *quasimodule*. It should be emphasized that we formulate our assumption without introducing inclusion relation and lattice operations. Using this assumption we are able to arrive in a purely arithmetic way to the Hadwiger-Minkowski operation; in fact we use the more convenient inner operations, having nice algebraic properties.

To make the above statements more precise, recall that, by definition, an abelian group (module) $(M, +)$ is an abelian semigroup with:

1. a unique null element 0, such that $a+0 = a$, for all $a \in M$, and
2. a unique opposite (additive inverse) operator opp:$M \longrightarrow M$, such that $a+\mathrm{opp}(a) = 0$, for all $a \in M$.

In addition, let us mention that if $(M, +)$ is a module, then for every $a, b \in M$:

1. the equation $a+x = b$ has a unique solution $x = b+\mathrm{opp}(a)$;
2. $a+x = b+x$ implies $a = b$ (cancellation law).

The semigroup $(S, +)$ has a null element and a binary operation exactly as a group has. Our additional assumption introduces in S a unary operation "negation", corresponding to the opposite operation in the group. Moreover, the semigroup satisfies the cancellation law (as a group does), and has inner operations which play the role of the operation subtraction in the group.

For simplicity we use the prefix "quasi-" for concepts related to S, and the prefix "pseudo-" (suggested in [Popova 1997]) for the corresponding concepts related to the set of factorized pairs $G = S^2/\!\sim$, discussed in Section 5.

By the familiar "classical" method, a quasimodule is isomorphically embedded into a special module, called "extended factor module". In a quasimodule we introduce multiplication by real scalar and define axiomatically a "quasilinear space" using the quasidistributive law as one of it's axioms. Under the classical embedding the quasidistributive law appears as a "pseudodistributive" law in the naturaly induced "pseudolinear space". It is demonstrated how certain "quasilinear" and "pseudolinear" algebraic equations can be solved; some rules for algebraic transformation of expressions are also given.

2 Quasimodules

Throughout the paper the term "module" means "additive abelian group"; "semimodule" means "additive abelian proper semigroup". Let $(S,+)$ be a semimodule with cancellation law (c.l.). We impose a special additional assumption on $(S,+)$, abstracted from the arithmetic properties of intervals and convex bodies. According to this assumption the semimodule S incorporates a module and the latter induces a natural operator over the semimodule. Namely, we shall assume that:

1. the semimodule S has a proper (nontrivial) submodule M;
2. the opposite operator in M is isomorphically extended over S.

The precise formulation of the above mentioned assumption follows:

M-assumption.

M1. There exists a submodule $(M,+)$ of $(S,+)$, such that:
  i) $M \neq \{0\}$;
  ii) M is maximal with respect to "$\subset$", that is for any other submodule M' of S we have $M' \subset M$;

M2. There exists a unique operator "negation" neg: $S \longrightarrow S$, such that:
  i) $\mathrm{neg}(A) = 0 \Longleftrightarrow A = 0$, for $A \in S$;
  ii) $\mathrm{neg}(\mathrm{neg}(A)) = A$, for $A \in S$;
  iii) $\mathrm{neg}(A+B) = \mathrm{neg}(A) + \mathrm{neg}(B)$, for $A, B \in S$;
  iv) $\mathrm{neg}(P) + P = 0$, for $P \in M$.

Remark. Since $(S,+)$ is assumed to be a proper semigroup (that is not a group itself) we have $M \subset S$, $M \neq S$. The condition $M \neq \{0\}$ where 0 denotes the null element of M, means that the module M is not trivial, i.e. M contains at least one element P, such that $P \neq 0$. Applied to a proper abelian semigroup S the M-assumption says that S includes a nontrivial module M which induces an operator "negation" on S.

The null of the group $(M,+)$ is also null of $(S,+)$, hence $(S,+)$ is a monoid, i. e. a semigroup with null element [MacLane and Birkhoff 1979].

The module $(M,+)$ is a group, hence there exists an opposite operator in M. As usually, we denote the opposite in M by "$-$", so that $(-P)+P=0$ for $P \in M$. Condition M2.iv) in the M-assumption can be written: $\mathrm{neg}(P) = -P$, for $P \in M$, showing that the restriction of "neg" to M coincides with the opposite "$-$" in M. To say it differently, property M2 means that "negation" is an automorphism in S which isomorphically extends "opposite" from M into S.

In the arithmetic for intervals, resp. convex bodies, the operator "neg" in S is traditionally denoted by the symbol "$-$". One motivation for this notation is that there is no opposite operator in $S \setminus M$, and in M the opposite and the restriction of negation coincide. Thus no confusion due to the use of the symbol "$-$" may occur within S. However, in Section 5 we shall extend S up to a factor group, where two different functions "opposite" and "negation" exist. Therefore we shall further denote negation by the special symbol "$\neg$" in order to avoid confusion with the opposite operator in the factor group extending S. As usually, the opposite operator is denoted by "$-$"; we also write $A+(-B) = A-B$ (and, sometimes, for more clarity, "$A -_{opp} B$", instead of $A-B$).

Definition 1. A semimodule (proper abelian semigroup) with c.l. satisfying the M-assumption will be called a *quasimodule* (*over* M) and will be denoted by $(S, M, +, \neg)$.

Note that a quasimodule $(S, M, +, \neg)$ has a binary, a unary and a nullary operation (addition, negation and null element), whereas a (general) semimodule is supposed to have only a binary operation. Thus the M-assumption substantially restricts the class of semimodules with c.l. We shall next demonstrate that in a quasimodule we can (in some cases) solve algebraic equations of the form $A+X=B$ "almost" as in a module.

3 Inner operations

Assume that $(S, S_0, +, \neg)$ is a quasimodule over a module S_0. We first introduce some concepts and notation.

Definition 2. Let $A, B \in S$. We say that A is a *summand* of B, symbolically: $A \leq_s B$, if there exists $C \in S$, such that $A+C=B$. If both $A \leq_s B$ and $B \leq_s A$ hold, we write $A =_s B$. We write $A <_s B$, if both $A \leq_s B$ and $A \neq_s B$ hold. If either $A \leq_s B$, or $B \leq_s A$ (or $A =_s B$) hold, we say that A, B are *s-comparable*. The set of all s-comparable pairs (A,B) is denoted by $G_s \subset S^2$.

In a quasimodule the element C in the above definition is unique. Indeed, in addition to $A+C=B$, assume $C \neq C'$, $A+C'=B$. From $A+C=B$, $A+C'=B$ it follows $A+C=A+C'$. By the c.l. we obtain the contradiction $C=C'$.

Remark. Note that for compact one-dimensional intervals every pair (A,B), $A, B \in S$, is s-comparable and the sets S^2 and G_s coincide, which is not true for arbitrary convex bodies.

We repeat the definitions of the symbols "$<_s, >_s, =_s, \leq_s$ once more verbally. For $(A, B) \in G_s$ we have:

i) $A <_s B$, if the equation $A + X = B$ is uniquely solvable, and equation $B + Y = A$ has no solution;

ii) $A >_s B$ ($B <_s A$), if $B + Y = A$ is uniquely solvable and $A + X = B$ has no solution;

iii) $A =_s B$ if both equations $A + X = B$ and $B + Y = A$ are uniquely solvable; in this case $X = -Y \in S_0$.

iv) "$\leq_s$" stands for the alternative "$<_s$" or "$=_s$".

Let $(S, S_0, +, \neg)$ be a quasimodule. For all $P, Q \in S_0$ we have $A =_s B$. Indeed, S_0 is a group and both equations $P + X = Q$ and $Q + Y = P$ have solutions, thereby $X = -Y \in S_0$. Assume now that $P \in S_0$, $P \neq 0$, $A \in S \setminus S_0$ (according to the M-assumption there exists at least one such P and at least one such A). We have $P =_s \neg P =_s 0$ (here, of course $\neg P = -P$). Also $A =_s A + P$ for all $P \in S_0$, due to $(A + P)\neg P = A + (P \neg P) = A$. Further, we have $A >_s P$. For, assume that $A =_s P$, that is $A + X = P$ and $P + Y = A$ have solutions. Then, from $(A + X) + (P + Y) = A + P$ it follows $X + Y = 0$ and $X = \neg Y \in S_0$. Then $A + X \in S_0$, which contradicts to $A \notin S_0$.

Denote by $X|_{A+X=B}$ the solution X of $A + X = B$. Note that we have $A =_s B$ if and only if $X|_{A+X=B} = \neg Y|_{B+Y=A} = -Y|_{B+Y=A} \in S_0$.

In a quasimodule S we introduce a partial binary operation "$+^-$" called *inner addition* for $A, B \in S$, such that $(A, \neg B) \in G_s$ (read: A and neg(A) are s-comparable).

Definition 3. Let $(S, S_0, +, \neg)$ be quasimodule. For $A, B \in S$ with $(A, \neg B) \in G_s$ the *inner sum* of A and B is given by:

$$A +^- B = \begin{cases} X|_{(\neg A)+X=B}, & \text{if } \neg A \leq_s B, \\ Y|_{(\neg B)+Y=A}, & \text{if } \neg B \leq_s A. \end{cases} \tag{4}$$

Note that $(A, \neg B) \in G_s$ implies $(\neg A, B) \in G_s$ (and vice verse). Note also that for $\neg A =_s B$ we have $X = Y$, therefore (4) is well defined.

Two more composite operations in $(S, S_0, +, \neg)$ will be used. *(Minkowski) subtraction* is a binary operation defined by $A \neg B = A + (\neg B)$, for all $A, B \in S$. *Inner subtraction* is a partial binary operation "$-^-$" defined for $(A, B) \in G_s$ by

$$A -^- B = A +^- (\neg B) = \begin{cases} \neg X \ |_{A+X=B}, & \text{if } A \leq_s B, \\ \ \ Y \ |_{B+Y=A}, & \text{if } B \leq_s A. \end{cases} \tag{5}$$

Proposition 4. *Let $(S, S_0, +, \neg)$ be a quasimodule. We have*

1) $A -^- A = A +^- (\neg A) = 0$ for all $A \in S$;

2) $A +^- B = B +^- A$, for $(A, \neg B) \in G_s$;

3) $\neg(A +^- B) = (\neg A) +^- (\neg B)$, for $(A, \neg B) \in G_s$;

4) $\neg(A -^- b) = (\neg A) -^- (\neg B)$ for $(A, B) \in G_s$;

5) $A -^- B = \neg(B -^- A)$ for $(A, B) \in G_s$;

6) $A + X = B$ and $A \leq_s B$ imply $X = B -^- A$;

7) $A \neg X = B$ and $A \leq_s B$ imply $X = A -^- B = \neg(B -^- A)$;

8) $(A +^- B) +^- C = A +^- (B +^- C)$ if $A \leq_s B$ and $C \leq_s B$.

Proof. Relations 1)–7) follow directly from (4) and (5). To prove 8) note that $A +^- B = X|_{\neg A+X=B}$, that is $\neg A + (A +^- B) = B$; similarly we have $\neg C + (B +^- C) = B$. Denote $(A +^- B) +^- C = D$ and $A +^- (B +^- C) = E$; to prove 8) we have to show that $D = E$. From $(A +^- B) +^- C = D$ it follows that either $D\neg B = A + C$ (if $\neg B \leq_s A + C$) or $D\neg(A + C) = B$ (if $A + C \leq_s \neg B$). Indeed, from $(A +^- B) +^- C = D$ we obtain one of the following two alternatives: a) either $\neg(A +^- B) + D = C$ which implies $A\neg(A +^- B) + D = A + C$, hence $D\neg B = A+C$; or b) $\neg C+D = A+^- B$ which implies $(\neg C+D)\neg A = (A+^- B)\neg A$, hence $D\neg(A+C) = B$. Similarly, from $A+^- (B+^- C) = E$ we obtain that either $\neg B+E = A+C$, or $E\neg(A+C) = B$. Consider the case $\neg B \leq_s A+C$. In this case we have both $D\neg B = A+C$ and $E\neg B = A+C$, which by the c.l. implies $D = E$. In the case $A + C \leq_s \neg B$ we have both $D\neg(A + C) = B$ and $E\neg(A + C) = B$, which again by the c.l. leads to $D = E$.

Quasimodules with T-assumption. In [Markov 1997] we postulate the following "trichotomy assumption" or "T-assumption", which is characteristic for intervals (but is not satisfied for general convex bodies):

T-assumption. For every $A, B \in S$ exactly one of $A <_s B$, $A =_s B$, or $A >_s B$ will hold.

Note that the T-assumption implies c. l. In [Markov 1997] we consider quasimodules satisfying the T-assumption (there called extended semigroups); we show that these special quasimodules can be endowed with multiplication by scalar and can be embedded in factor groups.

It will become clear in the sequence that the main results from [Markov 1997] hold for general quasimodules as well. Namely, we shall demonstrate that:

1. multiplication by scalar can be introduced in a quasimodule in exactly the same manner as in a quasimodule with T-assumption;
2. our basic embedding theorems for quasimodules with T-assumptions from [Markov 1997] are valid for general quasimodules, that is, in particular, for convex bodies.

Note that, in the case $G_s = S^2$ the inner addition is well defined for all $A, B \in S$; therefore inner addition is a binary operation in a quasimodule with T-assumption (and not a partial operation, as in a general quasimodule).

4 The quasilinear system

Denote the sign of the real number $p \in IR$ by $\sigma(p) \in \{+, -\}$, that is: $\sigma(p) = \{+, \text{ if } p \geq 0; -, \text{ if } p < 0\}$. In a quasimodule we introduce multiplication by scalar "$\cdot$" (the dot may be omitted) from the field IR as follows:

Definition 5. Let $(S, S_0, +, \neg)$ be a quasimodule. An operation defined for every pair p, A, with $p \in IR$, $A \in S$, denoted by $p \cdot A$ or pA, is called *multiplication by scalar*, if for $A, B \in S$, $p, q \in IR$, the following properties i)–v) are satisfied:

i) associativity of multiplication by scalar: $p(qA) = (pq)A$;
ii) first distributive law: $p(A + B) = pA + pB$;

iii) quasidistributive law:

$$(p+q)A = pA +^{\sigma(p)\sigma(q)} qA; \tag{6}$$

iv) $1 \cdot A = A$;
v) $(-1) \cdot P + P = 0$, for $P \in S_0$.

Remark. For $pq \geq 0$ equality (6) obtains the familiar form $(p+q)A = pA + qA$; for $pq < 0$ (6) obtains the form $(p+q)A = pA +^- qA$ with inner addition "$+^-$" defined by (4).

Proposition 6. *Let $(S, S_0, +, \neg)$ be a quasimodule with multiplication by scalar. For every $A \in S$ we have $\neg A = (-1) \cdot A$.*

Proof. We have to prove that in a quasimodule negation and multiplication by -1 coincide. Let us check if multiplication by -1 satisfies the properties M2 of the M-assumption. The first property M2.i): $(-1)A = 0$ iff $A = 0$ is easily verified, using that $p \cdot 0 = 0$ and $p \cdot A = 0$, $p \neq 0$ imply $A = 0$ (see Proposition 9). Property M2.ii) $(-1)(-1)A = A$ holds due to the associativity of multiplication by scalar. Property M2.iii): $(-1)(A+B) = (-1)A + (-1)B$ holds due to the quasidistributive law. Property M2.iv) is postulated in the definition for multiplication by scalar above (see the last fifth property): $(-1) \cdot P + P = 0$, for $P \in S_0$. Therefore multiplication by scalar is negation in the sense of the M-assumption. Since S is a quasimodule, negation is unique; therefore multiplication by -1 is negation in S. We thus proved that $\neg A = (-1) \cdot A$, that is $(-1) \cdot A$ is the unique negation in S.

Proposition 7. *Let $(S, S_0, +, \neg)$ be a quasimodule. For $A \in S$, $pq \geq 0$, we have $(pA, qA) \in G_s$.*

Proof. According to (6) multiplication by scalar satisfies for $pq \geq 0$ the equality $(p+q)A = pA + qA$. To show that $(pA, qA) \in G_s$ we have to check various cases for p and q. Let $p \geq q \geq 0$. Denote $p - q = r \geq 0$. By (6) we have $pA = (r+q)A = rA + qA \Longrightarrow (pA, qA) \in G_s$. The other cases are treated analogously.

Note that the inner addition "$+^-$" appearing in (6) in the case $pq < 0$ is defined if pA and qA are such that pA and $\neg(qA) = (-q)A$ are s-comparable. Due to Proposition 7 this is indeed the case, since p and $-q$ have same signs. Therefore, the expression in the right-hand side of (6) is well defined for *all* $p, q \in I\!R$ and $A \in S$.

A quasimodule $(S, S_0, +, \neg)$ endowed with multiplication by scalar will be denoted by $(S, S_0, +, I\!R, \cdot)$; we may omit the symbol for negation, since negation and multiplication by -1 coincide.

Definition 8. A quasimodule with multiplication by real scalar $(S, S_0, +, I\!R, \cdot)$ is called a *$I\!R$-quasimodule* (*over* S_0) or a *quasilinear (quasivector) system (over S_0 and $I\!R$)*. The elements of a quasilinear space are called *quasivectors*.

Remark. The term "quasilinear space" has been introduced in [Mayer 1968], [Mayer 1970]. Our quasilinear system is a special case of Mayer's quasilinear space, since the latter does not satisfy c.l. and M-assumption). As noted in [Ratschek 1975] Mayer's quasilinear space is too general and is not well suited for an effective description of interval spaces; same holds for spaces of convex bodies. Moreover, Mayer's system is "incomplete" in the sense that it is based on formula (3) and does not consider any rule for expressing $(p+q)A$ by means of pA and qA in the case $pq < 0$. The M-assumption permits the formulation of a general rule (6) for all $p, q \in I\!R$ and adds more algebraic structure necessary for the study of intervals and compact bodies. An important point is that the quasidistributive law (6) makes sense for all $A \in S$, $p, q \in I\!R$ (despite of the fact that the inner operation involved is a partial operation!). The notion "$I\!R$-semigroup with c.l.", used in [Ratschek and Schröder 1977] is better suited (it assumes c.l.), but is still too general (it lacks the M-assumption).

As we already mentioned, the established symbol for negation $-A = (-1) \cdot A$ in the arithmetic of intervals and convex bodies, may lead to confusion when passing to extended systems possessing an opposite operator to be considered in the next section; therefore we shall not use the symbol "$-$" to denote negation. On the other side, the advantages of introducing any new symbolic notation for the expression $(-1) \cdot A$ (such as the symbol "$\neg$") are doubtful; some readers may prefer not to use any new symbol for negation and write negation as $(-1) \cdot A$. Therefore we shall sometimes give in the sequence the expressions using negation twice: with the symbol "$\neg$" and without it, that is using $(-1) \cdot A$.

Proposition 9. *Let $(S, S_0, +, I\!R, \cdot)$ be a quasilinear space over $I\!R$. For all $p, q \in I\!R$ and for all $A, B, C \in S$ the following properties hold true:*

1. $\neg 0 = 0$, *i.e.* $(-1) \cdot 0 = 0$ *(quasivector zero);*
2. $p \cdot 0 = 0$;
3. $0 \cdot A = 0$;
4. $(p - q)A = pA -^{\sigma(p)\sigma(q)} qA$;
5. $p(A \neg B) = pA \neg pB$, *i.e.* $p(A + (-1) \cdot B) = pA + (-p) \cdot B$;
6. $p(A +^- B) = pA +^- pB$
7. $p(A -^- B) = pA -^- pB$
8. $pA = qA \Longrightarrow p = q$ *or* $A = 0$;
9. $pA = pB \Longrightarrow p = 0$ *or* $A = B$;
10. $pA = 0 \Longrightarrow p = 0$ *or* $A = 0$;
11. $A -^- A = 0$.

Proof. Relations 1)–11) are trivially verified. As example let us check relations 2), 10) and 11). Proof of 2). We have $p0 + 0 = p0 = p(0+0) = p0 + p0$, hence by the c.l. $p0 = 0$. Proof of 10). Let $pA = 0$. If $p \neq 0$, $A = 1 \cdot A = (p^{-1}p) \cdot A = p^{-1}(pA) = p^{-1}0 = 0$. Proof of 11). Setting $p = 1$, $q = -1$ in (6), implies $A +^- (\neg A) = A -^- A = 0$, as expected.

The quasidistributive law (6) permits to disclose brackets in expression of the form $(p+q)A$. However, (6) does not always permit to take the common quasivector A out of brackets in expressions of the form $pA + qA$ and $pA +^- qA$. Namely, for nondegenerate A (that is $A \in S \backslash S_0$) and real $pq < 0$ there is no real t such that $pA + qA = tA$; for $pq > 0$ there exist no real s such that $pA +^- qA = sA$.

Recall that we have $pA + qA = (p+q)A$ if $pq \geq 0$ and $pA +^- qA = (p+q)A$ if $pq \leq 0$. In the remaining cases we cannot use (6) directly. Nevertheless, we can solve with respect to X equations of the form $pX + qX = D$, $pX +^- qX = E$ for all $p, q \in IR$, $p^2 - q^2 \neq 0$. The next proposition summarizes the possible situations, related to these equations, and is easily verified.

Proposition 10. *The equation $pX +^\lambda qX = C$, for $p^2 - q^2 \neq 0$, $\lambda \in \{+,-\}$, has as solution $X = (p^2 - q^2)^{-1}(pC -^{(-\lambda)} qC)$.*

5 Embedding of a quasimodule into a group

Since every quasimodule $(S, S_0, +, \neg)$ is an abelian semigroup with c.l., $(S, +)$ can be isomorphically embedded in an abelian group (module) $(G, +)$ [Markov 1997], [Ratschek and Schröder 1977], [Rådström 1952]. Furthermore, G can be chosen so as to be minimal in the sense that if G' is any group in which S is embedded, then G is isomorphic to a subgroup of G' containing S. Such a minimal group can be obtained by the following familiar method (further referred as "classical").

According to the classical method, the set $G = S^2/\!\sim$ consists of all pairs $(A, B), A, B \in S$, factorized by the equivalence relation $\sim$: $(A, B) \sim (U, V) \Longleftrightarrow A + V = B + U$, for any $A, B, U, V \in S$. The equivalence class containing the pair (A', A'') will be denoted again by (A', A''). Addition in G defined by $(A, B) + (C, D) = (A + C, B + D)$ turns G into a group; the opposite element in G is $\mathrm{opp}(A, B) = -(A, B) = (B, A)$.

We subdivide the factorized set $G_s/\!\sim$ of s-comparable pairs into three disjoint subsets: $G_+ = \{(A, B) \mid B <_s A\}$, $G_- = \{(A, B) \mid A <_s B\}$, $G_0 = \{(A, B) \mid A =_s B\}$, so that $G = G_+ \bigcup G_0 \bigcup G_-$. The M-assumption implies that the sets G_+, G_0 and G_- are not empty. The set $G_s/\!\sim$ will be denoted again by G_s.

We can see that due to $A \geq_s 0$, $(A, 0) + (B, 0) = (A + B, 0)$, the semigroup $(S, +)$ is isomorphically embedded in $(G, +)$ under $\varphi : S \longrightarrow G_{+,0} = G_+ \bigcup G_0$ with $\varphi(A) \equiv (A, 0)$, $A \in S$. For $P \in S_0$ we have $\varphi(P) = (P, 0) = (0, -P)$, since $P + (-P) = 0$. The image of S under φ is $\varphi(S) = G_{+,0}$; moreover, we have $\varphi(S_0) = G_0$ and $\varphi(S_+) = G_+$, where $S_+ = S \setminus S_0$ and G_0 is the maximal subgroup of G. We may use a unique representation of the factorized pairs of s-comparable elements, by writing the elements of $G_{+,0}$ in the form $(A, 0)$ with $A \in S$, and those of G_- in the form $(0, B)$ with $B \in S_+$. The elements of G_0 are called *degenerate*, those of G_+ are *proper* and those of G_- are *improper*. We shall use lower case letters to denote the elements of G, e. g. $a = (A', A'')$. The function *type* (or *direction*) is defined by

$$\tau(a) = \begin{cases} +, & \text{if } a \in G_{+,0}, \\ -, & \text{if } a \in G_-. \end{cases}$$

We shall say that two elements of G are of *same type* if they either both belong to G_+, or both belong to G_-.

Remark. Using the function "type" we can present every element $a \in G_s$ in the form $(A; \tau(a))$ with a unique $A \in S$, called the "proper projection" of a, symbolically $A = \mathrm{pro}(a)$. Using such "pro-tau"-form the s-comparable pairs can be interpreted as "directed elements of S". By means of this method statements for

s-comparable pairs can be reformulated ("projected") as statements for elements of the original set S (for more detail, see [Markov 1996], [Markov 1997], where an isomorphism between the s-comparable pairs and the "pro-tau" elements is established and some applications are given).

An operator neg: $G \longrightarrow G$ satisfying the properties: N1) $\mathrm{neg}(a) = 0 \Longleftrightarrow a = 0$, $a \in G$; N2) $\mathrm{neg}(\mathrm{neg}(a)) = a$, $a \in G$; N3) $\mathrm{neg}(a + b) = \mathrm{neg}(a) + \mathrm{neg}(b)$, $a, b \in G$; N4) $\mathrm{neg}(p) + p = 0$ for $p \in G_0$; N5) $\mathrm{neg}(a) + a \neq 0$ for $a \in G \setminus G_0$, will be called "negation in G". It is easy to check that the operator $\mathrm{neg}(A, B) \equiv (\neg A, \neg B)$ is negation in G. Properties N1)–N4) show that negation in G isomorphically extends negation from the quasimodule S, resp. $G_{+,0}$.

Note that both "neg" and "opp" satisfy properties N1)–N4) in G, that is, N1–N4) remain true if we formally replace "opp" for "neg". Both "opp" and "neg" coincide on G_0. However, "neg" and "opp" are distinct on $G \setminus G_0$; indeed, the elements a and $\mathrm{neg}(a)$ for $a \in G \setminus G_0$ are of same type, whereas a and $\mathrm{opp}(a)$ are not. Thus "opp" and "neg" are two distinct isomorphic extensions of the operator "opp" from G_0 into G. Instead of N5) "opp" satisfies $\mathrm{opp}(a) + a = 0$, $a \in G$. The *symmetric* elements $\mathrm{neg}(a) + a$ form a subgroup of G [Markov 1997].

The operator dual: $G \longrightarrow G$ defined by $dual(A, B) = neg(opp(A, B)) = neg(B, A) = (\neg B, \neg A)$ satisfies: D1) $\mathrm{dual}(a) = 0 \Longleftrightarrow a = 0$, $a \in G$; D2) $\mathrm{dual}(\mathrm{dual}(a)) = a$, $a \in G$; D3) $\mathrm{dual}(a + b) = \mathrm{dual}(a) + \mathrm{dual}(b)$, $a, b \in G$; D4) $\mathrm{dual}(p) = p$, $p \in G_0$; D5) $\mathrm{dual}(a) + a \in G_0$ for $a \in G \setminus G_0$. Thus "dual" isomorphically extends the "identity" from S into G. Both "dual" and "identity" in G satisfy properties D1)–D4); they coincide on G_0 but for $a \in G \setminus G_0$, the elements a and $\mathrm{dual}(a)$ are not of same type. Hence "dual" and identity are two distinct isomorphic extensions of the identity from $G_0 = S_0$ into G; note that "identity" does not satisfy D5. In a factor module G generated by a quasimodule S using the classical method the operator "neg" will be denoted by "$\neg$" as we do in S. The factor module will be further denoted fully by $(G, G_0, +, \neg)$ to remind of the existence of a subgroup G_0 and a negation in G. Since G is a group, it has an opposite, and a "dual", which is a composite of "neg" and "opp". We shall symbolically write: dual $(a) = a_-$. We summarize the above arguments in the following proposition;

Proposition 11. *A quasimodule $(S, S_0, +, \neg)$ generates a module $(G, G_0, +, \neg)$ having the following properties:*

1) $(G, +)$ is the minimal isomorphic extension of $(S, +)$, unique up to isomorphism; $G_0 \cong S_0$ is the maximal proper submodule of G;

2) the operators "opp" and "neg" in G are isomorphic extensions of the opposite operator in G_0;

3) the identity in G_0 induces two isomorphic extensions in G: i) identity and ii) "dual", which is a composition of "opp" and "neg".

4) the automorphic operators opp, neg, dual are idempotent, i. e. for $a \in G$: $opp(opp(a)) = neg(neg(a)) = dual(dual(a)) = a$; symbolically: $-(-a) = \neg(\neg a) = (a_-)_- = a$;

5) the automorphic operators opp, neg, dual and identity form a Hamiltonian group. That is, we have for $a \in G$: $dual(a) = opp(neg(a)) = neg(opp(a))$; $opp(a) = neg(dual(a)) = dual(neg(a))$; $neg(a) = opp(dual(a)) = dual(opp(a))$. Symbolically: $dual(a) = -(\neg a) = \neg(-a)$; or: $dual(a) = -((-1) \cdot a) = (-1) \cdot (-a)$; $opp(a) = \neg(-a_-) = -(\neg a)_-$, etc.

Proposition 11 states that $(G, G_0, +, \neg)$ isomorphically extends $(S, S_0, +, \neg)$, and is unique up to isomorphism.

Definition 12. The unique minimal factor module $(G, G_0, +, \neg)$ induced by the quasimodule $(S, S_0, +, \neg)$ is called an *extended factor module over S*.

6 Embedding of a quasilinear system

According to Proposition 11 every quasimodule S can be isomorphically embedded in an extended factor module G with negation (and therefore with "dual" as well). We shall next extend the multiplication by scalar from $(S, S_0, +, I\!R, \cdot)$ into G, in order to embed isomorphically a quasilinear system into a system having group properties with respect to addition.

The following notation will be used: dual $(a) = a_-$, $a = a_+$; then a_λ is either a or dual(a) according to the value of $\lambda \in \{+, -\}$.

Proposition 13. *Let $(S, S_0, +, I\!R, \cdot)$ be a quasilinear space and let $(G, G_0, +, \neg)$ be a an extended factor module over S. Assume $A, B \in S$, $p, q \in I\!R$, $a, b \in G$. Then:*

i) the equality $p(A, B) = (pA, pB)$ isomorphically extends multiplication by scalar from S on G; multiplication by "-1" is negation in G ($\neg a = (-1)a, a \in G$);

ii) $p(qa) = (pq)a$, $p(a + b) = pa + pb$, $1a = a$;

iii) pseudodistributive law:

$$(p + q)a_{\sigma(p+q)} = pa_{\sigma(p)} + qa_{\sigma(q)},\ a \in G,\ p, q \in I\!R; \tag{7}$$

Proof. Proving i)–ii) presents no difficulties.To prove (7) we have to verify a number of cases. The case $\sigma(p)\sigma(q) = +$ is trivial. Let $\sigma(p)\sigma(q) = -$. Consider the subcase $p > 0, q < 0, p + q > 0 (p > -q)$. For this values (6) gives $(p + q)A = pA +^- qA$, which is equivalent to $(-q)A + (p + q)A = pA$. This leads to the following equality in G: $(-q)(A, 0) + (p + q)(A, 0) = p(A, 0)$ or $(p + q)(A, 0) = p(A, 0) -_{opp} (-q)(A, 0) = p(A, 0) + q(A, 0)_{\sigma(q)}$. In the last equality we have used that "opp" is a composition of "neg" abd "dual". The latter is exactly (7) since we have $(p + q)(A, 0)_{\sigma(p+q)} = p(A, 0)_{\sigma(p)} + q(A, 0)_{\sigma(q)}$. The rest of the cases are treated similarly.

The pseudodistributive law can be also written in the form: $(p + q)a = pa_\lambda + qa_\mu$, with $\lambda = \sigma(p)\sigma(p + q)$, $\mu = \sigma(q)\sigma(p + q)$.

Proposition 14. *1) For $a, b, x \in G$, $\xi \in I\!R$, $\xi \neq 0$, the equation $a + \xi x = b$ is equivalent to $x = \xi^{-1}(b + (\neg a_-)) = \xi^{-1}(b + (-a)) = \xi^{-1}(b -_{opp} a)$. 2)For $p, q \in I\!R$, $\lambda \in \{+, -\}$, $d \in G$, $s \equiv p^2 - q^2 \neq 0$, the equation $px + qx_\lambda = d$ has a unique solution $x = s^{-1}(pd + (-q)d_{-\lambda})_{\sigma(s)}$. (If $\lambda = \sigma(pq)$ using (7) we have: $x = (p + q)^{-1} d_{\sigma(1+q/p)}$.)*

We shall denote an extended factor module endowed with multiplication by scalar by $(G, G_0, +, I\!R, \cdot)$ omitting the "$\neg$" as special case of multiplication by scalar. The algebraic system $(G, G_0, +, I\!R, \cdot)$ is called $I\!R$-*pseudomodule (over G_0)* or *pseudolinear system (over G_0 and $I\!R$)*. Using this terminology we can state

Proposition 13 as: every quasilinear system can be isomorphically embedded in a pseudolinear system.

Let S be the set $I(I\!R^n)$ of all n-dimensional compact intervals on $I\!R^n$; in this case $S_0 = I\!R^n$, so that our quasilinear space is $(I(I\!R), I\!R^n, +, I\!R, \cdot)$. In Example 1 below we consider the case of one-dimensional intervals $n = 1$; in this case the T-assumption holds. The n-dimensional case is a special case of convex bodies; we consider the general case of convex bodies in Example 2.

Example 1. In the case of one-dimensional compact intervals on the real line we usually write $(I(I\!R), +, \cdot)$ instead of $(I(I\!R), I\!R, +, I\!R, \cdot)$. Consider the endpoint presentation: $A = [a^-, a^+] \in I(I\!R)$, $a^- < a^+$. Interval (Minkowski) addition in $I(I\!R)$: $A + B = \{x + y \mid x \in A, y \in B\}$ and negation: $\neg A = \{-x \mid x \in A\}$ are expressed end-pointwise by $A+B = [a^-, a^+]+[b^-, b^+] = [a^-+b^-, a^++b^+]$, resp., $\neg[a^-, a^+] = [-a^+, -a^-]$. The interval arithmetic system $(I(I\!R), +, \neg)$ is a quasimodule, satisfying the T-assumption, with $A \le_s B$ meaning $a^+ - a^- \le b^+ - b^-$. The inner sum of the intervals $[a^-, a^+]$, $[b^-, b^+]$ is the interval with end-points $a^- + b^+$ and $a^+ + b^-$, symbolically

$$[a^-, a^+] +^- [b^-, b^+] = \begin{cases} [a^- + b^+, a^+ + b^-], & \text{if } B \le_s A; \\ [a^+ + b^-, a^- + b^+], & \text{if } A <_s B. \end{cases}$$

Multiplication by scalar in $I(I\!R)$, given by

$$pA = \{px \mid x \in A\} = \begin{cases} [pa^-, pa^+], & \text{if } p \ge 0; \\ [pa^+, pa^-], & \text{if } p < 0, \end{cases}$$

satisfies the quasidistributive law (6); hence $(I(I\!R), +, \cdot)$ is a quasilinear system. Theorem 13 states that $(I(I\!R), +, \cdot)$ is isomorphically embedded into a pseudolinear system, which is a group with respect to "+" and satisfies the pseudodistributive law (7). The pseudovectors (also called *directed* or *generalized intervals*) can be expressed in the form $[a^-, a^+]$, $a^-, a^+ \in I\!R$ (no restriction $a^- \le a^+$ assumed). The operators "dual" and "opp" in the pseudolinear interval system are: $\mathrm{dual}[a^-, a^+] = [a^+, a^-]$, $\mathrm{opp}[a^-, a^+] = [-a^-, -a^+]$ [Kaucher 1977], [Markov 1996], [Markov 1997]. The directed intervals can be also presented in the "pro-tau" form: $[A; \alpha]$, $A \in I(I\!R), \alpha \in \{+, -\}$ [Markov 1995]; this form permits simple "projection" of results from the pseudolinear space of directed intervals to the quasilinear space of normal intervals.

Example 2. The class of all convex compact subsets of an Euclidean space $I\!E$ will be denoted by $\mathcal{K} = \mathcal{K}(I\!E)$. The elements of $\mathcal{K}$ are called *convex bodies*; see e.g. [Schneider 1993]. The properties of convex bodies imply that the system $(\mathcal{K}, I\!E, +, I\!R, \cdot)$ is a quasilinear space. Important relations in $\mathcal{K}$ are inclusion and the induced lattice operations. To turn $\mathcal{K}$ into complete lattice, one extends it by $I\!E$ (as a single element of $\mathcal{K}$) and by one more element $\emptyset$, called the empty set, satisfying $\emptyset + A = A + \emptyset = \emptyset + \emptyset = \emptyset$, $A \in \mathcal{K}$; $\alpha\emptyset = \emptyset$, $\alpha \in I\!R$.

Let $A, B \in \mathcal{K}$. The Hadwiger-Minkowski subtraction

$$A -_{HM} B = \bigcap_{b \in B} (A - b) \tag{8}$$

is introduced by H. Hadwiger [Hadwiger 1957]; an equivalent presentation is $A -_{HM} B = \{x \in I\!E \mid x + B \subset A\}$. Inner addition $A +^- B$ for $A, B \in \mathcal{K}$, is defined [Markov 1997a] by

$$A +^- B = \begin{cases} \bigcap_{b\in B} (A+b), & \text{if} \neq \emptyset, \\ \bigcap_{a\in A} (B+a), & \text{if} \neq \emptyset, \\ \emptyset, & \text{otherwise.} \end{cases}$$

(Note that if both intersections in the right-hand side are not empty, they coincide.) It is easy to see that $A +^- B = (A -_{HM} (\neg B)) \cup (B -_{HM} (\neg A))$. For the inner subtraction $A -^- B$, $A, B \in \mathcal{K}$, we have:

$$A -^- B \equiv A +^- (\neg B) = (A -_{HM} B) \cup (B -_{HM} A).$$

For every s-comparable pair $(A, B) \in G_s$ of convex bodies the Hadwiger-Minkowski difference (8) can be expressed by

$$A -_{HM} B = \begin{cases} Z|_{B+Z=A}, & \text{if } B \leq_s A, \\ \emptyset, & \text{if } A <_s B. \end{cases} \tag{9}$$

Comparing (5) and (9) we have for $(A, B) \in G_s$

$$A -^- B = \begin{cases} A -_{HM} B, & B \leq_s A, \\ \neg(B -_{HM} A), & A <_s B, \end{cases}$$

showing that the inner difference is a “symmetrized” Hadwiger-Minkowski difference. The inner operations satisfy the relations formulated in the present paper.

7 Conclusion

In this work we generalize our results for interval systems [Markov 1997] to hold for systems of convex bodies. We also formulate practical rules for algebraic transformation of expressions and solution of algebraic equations. We essentially show that all computational rules for intervals involving addition, subtraction, inner addition, inner subtraction and scalar multiplication, hold for (S-comparable pairs of) convex bodies as well.

For the interval case due to $G_s = G$ the inner addition is well defined operation in the quasimodule; for convex bodies inner addition is only partially defined. Nevertheless, it turns out that no difficulties arrise from this fact. Many other properties for intervals [Markov 1995] and convex bodies [Hadwiger 1957], [Markov 1997a], [Schneider 1993], not included here, are valid within the abstract framework given in this paper, as well. Inner addition of intervals is studied in [Markov 1977]–[Markov 1997]. Inner subtraction is related to Hadwiger-Minkowski subtraction $A -_{HM} B$; in the case of s-comparable A, B the latter satisfies the basic equality $(A -_{HM} B) + B = A$.

The M-assumption provides a suitable base for the abstract study of the arithmetic systems of intervals and convex bodies. Using the M-assumption we naturally introduce the inner addition (4), and formulate the quasidistributive law (6), arriving thus to the quasilinear and pseudolinear systems, which can be considered as generalisation of the familiar linear systems (with $S = S_0$). Calculations in a pseudolinear system $(G, G_0, +, I\!R, \cdot)$ are similar to those in a familiar linear system up to the following two main differences: i) in G we have four basic automorphisms ("neg", "opp", "dual" and "identity") against two ("opp" and "identity") in an usual linear system, and ii) a pseudo-distributive law involving the operator "dual" replaces the familiar second distributivity law. Based on the results in this work, specific rules for algebraic transformations and symbolic computations can be developed. Such results are a further step to the solution of algebraic problems involving intervals and convex bodies.

Acknowledgements

This work was partially supported by the Bulgarian National Science Fund under grant No. I-507/95.

References

[Hadwiger 1957] Hadwiger, H.: "Vorlesungen über Inhalt, Oberfäache und Isoperimetrie"; Springer (1957).

[Kaucher 1977] Kaucher, E.: "Algebraische Erweiterungen der Intervallrechnung unter Erhaltung der Ordnungs- und Verbandstrukturen"; Computing Suppl., 1 (1977), 65–79.

[MacLane and Birkhoff 1979] MacLane, S.; Birkhoff, G.: "Algebra", 2nd Ed.; Macmillan, New York (1979).

[Markov 1977] Markov, S.: "A non-standard subtraction of intervals"; Serdica, 3 (1977), 359–370.

[Markov 1995] Markov, S.: "On Directed Interval Arithmetic and its Applications"; J. UCS, 1, 7 (1995), 510–521.

[Markov 1996] Markov, S.: "On the Foundations of Interval Arithmetic"; Scientific Computing and Validated Numerics (G. Alefeld et al., eds.); Mathematical Research, 90, Akademie Verlag (1996), 307–313.

[Markov 1997] Markov, S.: "Isomorphic Embedding of Abstract Interval Systems"; Reliable Computing, 3 (1997), 199–207.

[Markov 1997a] Markov, S.: "On the Algebraic Properties of Convex Bodies"; submitted to Serdica.

[Mayer 1968] Mayer, O.: "Über Eigenschaften von Intervallprozessen,"; ZAMM, 48 (1968), T86–T87.

[Mayer 1970] Mayer, O.: "Algebraische und metrische Strukturen in der Intervallrechnung und einige Anwendungen"; Computing 5 (1970), 144–162.

[Popova 1997] Popova E.: "Algebraic Solutions to Some Interval Equations"; submitted to J. UCS (1997).

[Rådström 1952] Rådström, H.: "An Embedding Theorem for Spaces of Convex Sets"; Proc. Amer. Math. Soc. 3 (1952), 165–169.

[Ratschek 1975] Ratschek, H.: "Nichtnumerische Aspekte der Intervallmathematik"; Interval Mathematics (Ed. K. Nickel, Lecture Notes in Computer Science, 29, Springer, 1975.

[Ratschek and Schröder 1977] Ratschek, H.; G. Schröder: "Representation of semigroups as systems of compact convex sets"; Proc. Amer. Math. Soc. 65 (1977), 24–28.

[Schneider 1993] Schneider, R.: "Convex Bodies: The Brown-Minkowski Theory"; Cambridge Univ. Press (1993).