Preprint of an article published in *International Journal of Algebra and Computation* (2014), DOI: 10.1142/S0218196714500027.
http://www.worldscientific.com/worldscinet/ijac

RECONSTRUCTING MULTISETS OVER COMMUTATIVE GROUPOIDS AND AFFINE FUNCTIONS OVER NONASSOCIATIVE SEMIRINGS

ERKKO LEHTONEN

Abstract. A reconstruction problem is formulated for multisets over commutative groupoids. The cards of a multiset are obtained by replacing a pair of its elements by their sum. Necessary and sufficient conditions for the reconstructibility of multisets are determined. These results find an application in a different kind of reconstruction problem for functions of several arguments and identification minors: classes of linear or affine functions over nonassociative semirings are shown to be weakly reconstructible. Moreover, affine functions of sufficiently large arity over finite fields are reconstructible.

1. Introduction

Generally speaking, a reconstruction problem asks whether a mathematical object can be recovered from partial information. The kind of reconstruction problems we discuss in this paper fall into the following general scheme: given a combinatorial object, we apply a certain operation to its elements in all possible ways, and we ask whether the initially given object is uniquely determined (up to some kind of isomorphism) by the collection of these derived objects (which are called the cards of the object). Perhaps one of the most famous reconstruction problems is the following: Is every graph uniquely determined, up to isomorphism, by the collection of its subgraphs obtained by deleting a single vertex? It was conjectured by Kelly [5] (see also Ulam's problem book [12]) that the answer is positive, provided that the graph has at least three vertices. While the conjecture has been shown to hold for various classes of graphs, in full generality it remains an important open problem in graph theory.

In this paper we consider two different reconstruction problems. The first one deals with multisets over a commutative groupoid. The cards of a multiset M are the multisets obtained from M by replacing a pair of its elements by their sum. We find necessary and sufficient conditions for a multiset to be reconstructible in this setting. Reconstructibility depends on the cardinality and the form of a multiset and also on the underlying groupoid.

The reconstruction problem for multisets arose from a completely different reconstruction problem that was posed and studied in [7]. Here, the objects are functions of several arguments, and the cards of a function $f\colon A^n \to B$ are the $\binom{n}{2}$ identification minors of f, i.e., the $(n-1)$-ary functions obtained from f by identifying a pair of its arguments. The special case of affine functions over semirings reduces to the reconstruction problem for multisets over commutative groupoids. As an

application of our solution to the reconstruction problem for multisets, we show that classes of affine or linear functions over nonassociative semirings are weakly reconstructible. Moreover, affine functions of sufficiently large arity over finite fields are reconstructible.

A function $f\colon A^n \to B$ is called a minor of another function $g\colon A^m \to B$ if there exists a map $\sigma\colon \{1,\dots,m\} \to \{1,\dots,n\}$ such that $f(a_1,\dots,a_n) = g(a_{\sigma(1)},\dots,a_{\sigma(m)})$ for all $a_1,\dots,a_n \in A$. New discoveries – either positive or negative – about the reconstruction problem for functions and identification minors will shed some light on the minor relation, a topic that has attracted the attention of several researchers over the past years (see, e.g., [1, 2, 3, 4, 8, 10, 13, 14, 15]).

2. Preliminaries

We follow the standard terminology and notation of abstract algebra, as found, e.g., in [6, 9].

For a positive integer n, the set $\{1,\dots,n\}$ is denoted by $[n]$. The set of all 2-element subsets of $[n]$ is denoted by $\binom{n}{2}$. The set $\{0,1,2,\dots\}$ of nonnegative integers is denoted by $\mathbb{N}$.

A *finite multiset* M over a set X is a map $\mathbf{1}_M\colon X \to \mathbb{N}$, called a *multiplicity function,* such that the set $\{x \in X : \mathbf{1}_M(x) \neq 0\}$ is finite. We will only discuss finite multisets, and we will refer to them simply as *multisets.* For a finite multiset M, the sum $\sum_{x\in X} \mathbf{1}_M(x)$ is a well-defined natural number, and it is called the *cardinality* of M and denoted by $|M|$. We refer to a multiset of cardinality n as an *n-multiset.* For each $x \in X$, the number $\mathbf{1}_M(x)$ is called the *multiplicity* of x in M. We write $x \in M$ if $\mathbf{1}_M(x) \geq 1$. A multiset M is a *submultiset* of M', denoted $M \subseteq M'$, if $\mathbf{1}_M(x) \leq \mathbf{1}_{M'}(x)$ for all $x \in X$. The *empty multiset* $\emptyset$ is given by the multiplicity function $\mathbf{1}_\emptyset(x) = 0$ for all $x \in X$.

We may represent a finite multiset M as a list enclosed in angle brackets where each element $x \in X$ occurs $\mathbf{1}_M(x)$ times, e.g., $\langle 0,0,0,1,1,2\rangle$. Also, if $(a_i)_{i\in I}$ is a finite indexed family of elements of X, then we will write $\langle a_i : i \in I\rangle$ to denote the multiset in which the multiplicity of each $x \in X$ equals $|\{i \in I : a_i = x\}|$.

Let M and M' be finite multisets over X. The *multiset sum* $M \uplus M'$, the *difference* $M \setminus M'$, and the *intersection* $M \cap M'$ of M and M' are defined by the multiplicity functions

$$\begin{aligned}\mathbf{1}_{M\uplus M'}(x) &= \mathbf{1}_M(x) + \mathbf{1}_{M'}(x),\\ \mathbf{1}_{M\setminus M'}(x) &= \max(\mathbf{1}_M(x) - \mathbf{1}_{M'}(x), 0),\\ \mathbf{1}_{M\cap M'}(x) &= \min(\mathbf{1}_M(x), \mathbf{1}_{M'}(x)).\end{aligned}$$

3. Reconstruction problem for multisets over commutative groupoids

In this section, we formulate a reconstruction problem for multisets over commutative groupoids, and we completely characterize the reconstructible multisets. We will conclude the section with some open problems.

3.1. **Reconstruction problem for multisets.** Let $(G;+)$ be a commutative groupoid. Let n be an integer at least 2. Let M be a multiset of cardinality n over G. Fix an n-tuple $(m_1,\dots,m_n) \in G^n$ satisfying $M = \langle m_1,\dots,m_n\rangle$. For each $I \in \binom{n}{2}$, let $M_I := M \setminus \langle m_{\min I}, m_{\max I}\rangle \uplus \langle m_{\min I} + m_{\max I}\rangle$. The *cards* of

M are the multisets M_I, for each $I \in \binom{n}{2}$, and the *deck* of M is the multiset $\operatorname{deck} M := \langle M_I : I \in \binom{n}{2} \rangle$. (It is irrelevant which particular tuple $(m_1, \ldots, m_n)$ is chosen for a given M. Any valid choice will give rise to the same deck.)

A multiset M is *reconstructible* if for all multisets M' over G the condition $\operatorname{deck} M = \operatorname{deck} M'$ implies $M = M'$.

We have now all the necessary definitions for our discussion, and we can formulate a reconstruction problem for multisets over commutative groupoids. Is every multiset over a commutative groupoid reconstructible? If not, which multisets are reconstructible and which ones are not? Does the answer depend on the underlying groupoid?

Examples 3.1–3.4 below illustrate that the answer to our first question is negative: not every multiset over a commutative groupoid is reconstructible. The latter two questions will be answered later in this paper. It will turn out that these examples are exhaustive; there is no other nonreconstructible multiset over any commutative groupoid than the ones described in Examples 3.1–3.4.

Example 3.1. Let $(G; +)$ be a commutative groupoid with elements r, s, t, u, v satisfying $x + u = v$ and $x + v = u$ for all $x \in \{r, s, t\}$ and $r + s = s$, $s + t = t$, $t + r = r$. Let $M = \langle r, s, t, u \rangle$, $M' = \langle r, s, t, v \rangle$. If $u \neq v$, then $M \neq M'$ but

$$\operatorname{deck} M = \operatorname{deck} M' = \langle \langle r, s, u \rangle, \langle r, t, u \rangle, \langle s, t, u \rangle, \langle r, s, v \rangle, \langle r, t, v \rangle, \langle s, t, v \rangle \rangle.$$

Note that either r, s and t are pairwise distinct or $r = s = t$. For, assume that $r = s$. Then $t = s + t = r + t = r$, whence $r = s = t$. A similar argument shows that $r = t$ or $s = t$ implies $r = s = t$.

If r, s and t are pairwise distinct, then $r + (s + t) = r \neq t = (r + s) + t$, i.e., $(G; +)$ is not associative. If $r = s = t$ and $u \neq v$, then $r + (r + u) = u \neq v = (r + r) + u$, i.e., $(G; +)$ is not associative and not even alternative. (A binary operation is *left alternative* if it satisfies the identity $x(xy) = (xx)y$ and *right alternative* if it satisfies the identity $y(xx) = (yx)x$. An operation is *alternative* if it is both left and right alternative. Alternativity is a weaker form of associativity.)

Example 3.2. Let $(G; +)$ be a commutative groupoid with elements r, s, t satisfying $r + (r + s) = s$, $r + (r + t) = t$ and $(r + s) + (r + t) = s + t$. Let $M = \langle r, s, t \rangle$, $M' = \langle r, r + s, r + t \rangle$. Then

$$\operatorname{deck} M = \operatorname{deck} M' = \langle \langle r, s + t \rangle, \langle s, r + t \rangle, \langle t, r + s \rangle \rangle.$$

Furthermore, if $\{r + s, r + t\} \neq \{s, t\}$, then $M \neq M'$.

Note that if $(G; +)$ is a Boolean group (a group in which every nonneutral element has order 2), then the above conditions are satisfied by all elements $r, s, t \in G$. Furthermore, if r is not neutral and $r + s \neq t$, then $M \neq M'$.

Example 3.3. Let $(G; +)$ be a commutative groupoid with elements r, s, t satisfying $(r + s) + (r + t) = r$, $(r + s) + (s + t) = s$ and $(r + t) + (s + t) = t$. Let $M = \langle r, s, t \rangle$, $M' = \langle r + s, r + t, s + t \rangle$. Then

$$\operatorname{deck} M = \operatorname{deck} M' = \langle \langle r, s + t \rangle, \langle s, r + t \rangle, \langle t, r + s \rangle \rangle,$$

but M and M' are not necessarily equal.

Note that if $(G; +)$ is a monoid with neutral element 0, then the above conditions are satisfied by all elements $r, s, t \in G$ such that $r + s + t = 0$.

Example 3.4. Let $(G;+)$ be a commutative groupoid with elements r, s, t, u satisfying $r+s=t+u$ and $\{r,s\}\neq\{t,u\}$. Let $M=\langle r,s\rangle$, $M'=\langle t,u\rangle$. Then $M\neq M'$ but $\operatorname{deck} M=\operatorname{deck} M'=\langle\langle r+s\rangle\rangle$.

3.2. **The solution to the reconstruction problem for multisets.** We are going to show that a multiset over a commutative groupoid is reconstructible if and only if it is not any one of the multisets described in Examples 3.1–3.4. In our approach to characterizing the reconstructible multisets, we will make good use of the collection of all elements in all cards of a multiset, as it reveals plenty of information about the multiset itself. Let M be a multiset of cardinality n over a commutative groupoid $(G;+)$. Denote $\widetilde{M}:=\biguplus_{I\in\binom{n}{2}}M_I$, and denote $N_M(x):=\mathbf{1}_{\widetilde{M}}(x)$ for each $x\in G$.

Lemma 3.5. *Let M be a multiset of cardinality n over G. Then $N_M(x)=\mathbf{1}_M(x)\cdot\binom{n-1}{2}+\delta_M(x)$ for some $\delta_M\colon G\to\mathbb{N}$ satisfying $\sum_{x\in G}\delta_M(x)=\binom{n}{2}$.*

Proof. Fix an n-tuple $(m_1,\ldots,m_n)$ satisfying $M=\langle m_1,\ldots,m_n\rangle$ and for each $I\in\binom{n}{2}$, let $M_I:=M\setminus\langle m_{\min I},m_{\max I}\rangle\uplus\langle m_{\min I}+m_{\max I}\rangle$. Let us count the number of times each element of G occurs in the various cards of M. For each $i\in[n]$, there is an occurrence of m_i (that has not yet been counted) in M_I for every $I\in\binom{n}{2}$ such that $i\notin I$. Additionally, for each $I\in\binom{n}{2}$, there is an occurrence of $m_{\min I}+m_{\max I}$ in M_I. In other words, each occurrence of x in M contributes $\binom{n-1}{2}$ to the number $\mathbf{1}_{\widetilde{M}}(x)$, and each $I\in\binom{n}{2}$ contributes 1 to the number $\mathbf{1}_{\widetilde{M}}(m_{\min I}+m_{\max I})$. Let $\delta_M\colon G\to\mathbb{N}$ be the map given by the rule $\delta_M(x)=|\{I\in\binom{n}{2}:m_{\min I}+m_{\max I}=x\}|$. Then clearly $\sum_{x\in G}\delta_M(x)=\binom{n}{2}$ and we have $\mathbf{1}_{\widetilde{M}}(x)=\mathbf{1}_M(x)\cdot\binom{n-1}{2}+\delta_M(x)$ for all $x\in G$. □

Lemma 3.6. *Assume that $n\geq 4$, and let M and M' be multisets of cardinality n over G. Assume that $N_M(x)=N_{M'}(x)$ for all $x\in G$ and there exists $y\in G$ such that $N_M(y)$ is not a multiple of $\binom{n-1}{2}$. Then there exist elements $a,b\in G$ such that $M'=M\setminus\langle a\rangle\uplus\langle b\rangle$.*

Proof. If $M=M'$, then the claim clearly holds with $a=b$ for any $a\in M$. Assume that $M\neq M'$. Then there exist distinct elements a and b of G such that $\mathbf{1}_M(a)\neq\mathbf{1}_{M'}(a)$ and $\mathbf{1}_M(b)\neq\mathbf{1}_{M'}(b)$.

Observe that $\binom{n-1}{2}<\binom{n}{2}\leq 2\cdot\binom{n-1}{2}$ whenever $n\geq 4$ and the second inequality holds with equality if and only if $n=4$. By Lemma 3.5, there exist maps $\delta_M,\delta_{M'}\colon G\to\mathbb{N}$ such that $N_M(x)=\mathbf{1}_M(x)\cdot\binom{n-1}{2}+\delta_M(x)$ and $N_{M'}(x)=\mathbf{1}_{M'}(x)\cdot\binom{n-1}{2}+\delta_{M'}(x)$ for all $x\in G$ and $\sum_{x\in G}\delta_M(x)=\binom{n}{2}=\sum_{x\in G}\delta_{M'}(x)$. The assumption that $N_M(y)$ is not a multiple of $\binom{n-1}{2}$ implies that $\delta_M(x)\geq\binom{n-1}{2}$ for at most one $x\in G$ and $\delta_M(x)<2\cdot\binom{n-1}{2}$ for all $x\in G$; similarly $\delta_{M'}(x)\geq\binom{n-1}{2}$ for at most one $x\in G$ and $\delta_{M'}(x)<2\cdot\binom{n-1}{2}$ for all $x\in G$. We may assume, without loss of generality, that $\delta_M(a)<\binom{n-1}{2}$. This implies that $\mathbf{1}_{M'}(a)=\mathbf{1}_M(a)-1$ and $\delta_{M'}(a)=\delta_M(a)+\binom{n-1}{2}\geq\binom{n-1}{2}$. This in turn implies that $\delta_{M'}(x)<\binom{n-1}{2}$ for all $x\in G\setminus\{a\}$; in particular, $\delta_{M'}(b)<\binom{n-1}{2}$. Consequently, $\mathbf{1}_M(b)=\mathbf{1}_{M'}(b)-1$ and $\delta_M(b)=\delta_{M'}(b)+\binom{n-1}{2}\geq\binom{n-1}{2}$. It also follows that $\mathbf{1}_M(x)=\mathbf{1}_{M'}(x)$ for all $x\in G\setminus\{a,b\}$ (for, if there existed an element $c\in G\setminus\{a,b\}$ such that $\mathbf{1}_M(c)\neq\mathbf{1}_{M'}(c)$, then this would imply, similarly as above, that $\delta_M(c)\geq\binom{n-1}{2}$, which would contradict the fact that there is at most one $x\in G$ such that $\delta_M(x)\geq\binom{n-1}{2}$). We

conclude that $\mathbf{1}_{M'}(a) = \mathbf{1}_M(a) - 1$, $\mathbf{1}_{M'}(b) = \mathbf{1}_M(b) + 1$ and $\mathbf{1}_{M'}(x) = \mathbf{1}_M(x)$ for all $x \in G \setminus \{a, b\}$. In other words, $M' = M \setminus \langle a \rangle \uplus \langle b \rangle$. □

Theorem 3.7. *Assume that $(G; +)$ is a commutative groupoid, and M and M' are multisets over G with $|M| = |M'| \geq 5$. Then* $\operatorname{deck} M = \operatorname{deck} M'$ *if and only if $M = M'$.*

Proof. Let n be the common cardinality of M and M'. It is clear that if $M = M'$, then $\operatorname{deck} M = \operatorname{deck} M'$. For the converse implication, assume that $\operatorname{deck} M = \operatorname{deck} M'$. Then clearly $\widetilde{M} = \widetilde{M'}$, so $N_M(x) = N_{M'}(x)$ for all $x \in G$. Since $\sum_{x \in G} \delta_M(x) = \binom{n}{2}$ and $\binom{n-1}{2} < \binom{n}{2} < 2 \cdot \binom{n-1}{2}$ holds whenever $n \geq 5$, there exists $y \in G$ such that $N_M(y)$ is not a multiple of $\binom{n-1}{2}$. By Lemma 3.6, there exist $a, b \in G$ such that $M' = M \setminus \langle a \rangle \uplus \langle b \rangle$, say, $M = \langle m_1, \ldots, m_{n-1}, a \rangle$, $M' = \langle m_1, \ldots, m_{n-1}, b \rangle$ for some $m_1, \ldots, m_{n-1} \in G$.

Let us count the number of times each element of G occurs in the multisets $\widetilde{M}$ and $\widetilde{M'}$. Both multisets contain $\binom{n-1}{2}$ occurrences of m_i for each $i \in [n-1]$ and one occurrence of $m_{\min I} + m_{\max I}$ for each $I \in \binom{n}{2}$ such that $n \notin I$. The remaining elements of $\widetilde{M}$ are $\binom{n-1}{2}$ occurrences of a and one occurrence of $m_i + a$ for each $i \in [n-1]$; while the remaining elements of $\widetilde{M'}$ are $\binom{n-1}{2}$ occurrences of b and one occurrence of $m_i + b$ for each $i \in [n-1]$. Since $\binom{n-1}{2} > n - 1$ whenever $n \geq 5$, the equality $\widetilde{M} = \widetilde{M'}$ may hold only if $a = b$. We conclude that $M = M'$. □

Theorem 3.8. *Assume that $(G; +)$ is a commutative groupoid. Let M and M' be multisets of cardinality 4 over G. Then* $\operatorname{deck} M = \operatorname{deck} M'$ *if and only if one of the following conditions holds:*

(i) *$M = M'$.*
(ii) *$M = \langle r, s, t, u \rangle$ and $M' = \langle r, s, t, v \rangle$ for some elements $r, s, t, u, v \in G$ satisfying $x + u = v$ and $x + v = u$ for all $x \in \{r, s, t\}$ and $r + s = s$, $s + t = t$, $t + r = r$.*

Proof. Let $n = 4$. Then $\binom{n-1}{2} = 3 = n - 1$. It is clear that if $M = M'$, then $\operatorname{deck} M = \operatorname{deck} M'$. If condition (ii) holds, then $\operatorname{deck} M = \operatorname{deck} M'$, as shown in Example 3.1. For the converse implication, assume that $\operatorname{deck} M = \operatorname{deck} M'$. Then obviously $\widetilde{M} = \widetilde{M'}$ and $N_M(x) = N_{M'}(x)$ for all $x \in G$.

Assume first that there is $y \in G$ such that $N_M(y)$ is not a multiple of $\binom{n-1}{2}$. By Lemma 3.6, there exist elements $u, v \in G$ such that $M' = M \setminus \langle u \rangle \uplus \langle v \rangle$. If $u = v$, then $M = M'$ and we are done. Assume thus that $u \neq v$. Then $M = \langle r, s, t, u \rangle$ and $M' = \langle r, s, t, v \rangle$ for some $r, s, t \in G$, and the cards of M and M' are

$$\begin{aligned}
M_{12} &= \langle r + s, t, u \rangle, & M'_{12} &= \langle r + s, t, v \rangle, \\
M_{13} &= \langle r + t, s, u \rangle, & M'_{13} &= \langle r + t, s, v \rangle, \\
M_{23} &= \langle s + t, r, u \rangle, & M'_{23} &= \langle s + t, r, v \rangle, \\
M_{14} &= \langle r + u, s, t \rangle, & M'_{14} &= \langle r + v, s, t \rangle, \\
M_{24} &= \langle s + u, r, t \rangle, & M'_{24} &= \langle s + v, r, t \rangle, \\
M_{34} &= \langle t + u, r, s \rangle, & M'_{34} &= \langle t + v, r, s \rangle.
\end{aligned}$$

We must have $r + u = s + u = t + u = v$ and $r + v = s + v = t + v = u$. (Otherwise we would have $\widetilde{M} \neq \widetilde{M'}$, a contradiction.) Furthermore, r, s and t are

not all equal. (For, if $r = s = t$, then $r + s = r + t = s + t$ and $N_M(x)$ would be a multiple of $\binom{n-1}{2}$ for all $x \in G$, a contradiction.)

Since $\operatorname{deck} M = \operatorname{deck} M'$, there exists a one-to-one correspondence between the cards of M and the cards of M'. We are going to determine the possible correspondences. Observe first that $M_I \neq M'_I$ for all $I \in \binom{n}{2}$. Let us now focus on the card M_{14} of M.

Suppose first that $M_{14} = M'_{24}$, i.e., $\langle v, s, t\rangle = \langle u, r, t\rangle$. This implies that $r = v$ and $s = u$. Then $M_{13} = \langle u, u, u\rangle$, and this may correspond only to $M'_{14} = \langle u, u, t\rangle$ (because the other M'_{ij} contain v). Thus, $t = u$. But then every card of M contains u, so no card of M can be equal to $M'_{23} = \langle v, v, v\rangle$, and we have reached a contradiction. We conclude that $M_{14} \neq M'_{24}$; in a similar way, we can deduce also that $M_{24} \neq M'_{34}$ and $M_{34} \neq M'_{14}$.

Suppose then that $M_{14} = M'_{34}$, i.e., $\langle v, s, t\rangle = \langle u, r, s\rangle$. This implies that $r = v$ and $t = u$. A similar argument as above (now $M_{12} = \langle u, u, u\rangle$, $M'_{23} = \langle v, v, v\rangle$) leads to a contradiction. We conclude that $M_{14} \neq M'_{34}$; similarly, $M_{24} \neq M'_{14}$ and $M_{34} \neq M'_{24}$.

Suppose then that $M_{14} = M'_{23}$, i.e., $\langle v, s, t\rangle = \langle s + t, r, v\rangle$. This implies that $\{s, t\} = \{s+t, r\}$, and we must have $\{M_{24}, M_{34}\} = \{M'_{12}, M'_{13}\}$. If $M_{24} = M'_{12}$ and $M_{34} = M'_{13}$, then $\{r, t\} = \{r + s, t\}$ and $\{r, s\} = \{r + t, s\}$. Consequently, $r = r + s$ and $r = r + t$. From the equality $\{s, t\} = \{s + t, r\}$ we get that $s = s + t$ and $t = r$; or $s = r$ and $t = s + t$. In either case, it follows that $r = s = t$, a contradiction. If $M_{24} = M'_{13}$ and $M_{34} = M'_{12}$, then $\{r, t\} = \{r + t, s\}$ and $\{r, s\} = \{r + s, t\}$. By these equalities and by the equality $\{s, t\} = \{s + t, r\}$, we have $r = s$ or $r = t$; and $s = r$ or $s = t$; and $t = r$ or $t = s$. It follows that $r = s = t$, again a contradiction. We conclude that $M_{14} \neq M'_{23}$; similarly, $M_{24} \neq M'_{13}$ and $M_{34} \neq M'_{12}$.

Consider then the case that $M_{14} = M'_{12}$, i.e., $\langle v, s, t\rangle = \langle r + s, t, v\rangle$. Then we must have $M_{24} = M'_{23}$ and $M_{34} = M'_{13}$, i.e., $\langle v, r, t\rangle = \langle s + t, r, v\rangle$ and $\langle v, r, s\rangle = \langle r + t, s, v\rangle$. It follows that $r + s = s$, $s + t = t$, $t + r = r$. Therefore, condition (ii) holds.

Finally, consider the case that $M_{14} = M'_{13}$, i.e, $\langle v, s, t\rangle = \langle r + t, s, v\rangle$. A similar argument as in the previous case shows that $r+t = t$, $t+s = s$, $s+r = r$. Swapping the labels of the elements r and s, we see that condition (ii) holds. This completes the case analysis.

We have been working under the assumption that there is $y \in G$ such that $N_M(y)$ is not a multiple of $\binom{n-1}{2}$. Now suppose that this is no longer so, i.e., $N_M(x)$ is a multiple of $\binom{n-1}{2}$ for all $x \in G$. Then $\widetilde{M} = \widetilde{M'} = H \uplus H \uplus H$, where $H = M \uplus E = M' \uplus E'$ and $|E| = |E'| = 2$. If $M = \langle m_1, m_2, m_3, m_4\rangle$, then $E \uplus E \uplus E = \langle m_{\min I} + m_{maxI} : I \in \binom{n}{2}\rangle$; similarly for M' and E'. It thus holds that $x + y \in E$ whenever $\langle x, y\rangle \subseteq M$ and $x + y \in E'$ whenever $\langle x, y\rangle \subseteq M'$. Each one of the elements of E arises in three different ways as a sum of two elements of M; each one of the elements of E' arises in three different ways as a sum of two elements of M'.

We have several possibilities concerning the 6-multiset H and its possible partitions into a 4-multiset M and a 2-multiset E (which we will refer to as $(4, 2)$-*partitions* of H). The remainder of this proof is an analysis of the different cases that may arise. For easy reference, these cases are summarised in Table 1, in which we also present the deck of each multiset M considered. The different configurations (M, E) will be referred to as "types", which are labeled with codes of the

H	$\langle a,b,c,d,e,f\rangle$	$\langle a,a,b,c,d,e\rangle$			$\langle a,a,b,b,c,d\rangle$	
type	I.1	II.1	II.2	II.3	III.1	III.2
M	$\langle\alpha,\beta,\gamma,\delta\rangle$	$\langle a,a,\beta,\gamma\rangle$	$\langle a,\beta,\gamma,\delta\rangle$	$\langle b,c,d,e\rangle$	$\langle\alpha,\alpha,\beta,\gamma\rangle$	$\langle a,b,c,d\rangle$
E	$\langle\epsilon,\zeta\rangle$	$\langle\delta,\epsilon\rangle$	$\langle a,\epsilon\rangle$	$\langle a,a\rangle$	$\langle\beta,\delta\rangle$	$\langle a,b\rangle$
deck	$\langle\alpha+\beta,\gamma,\delta\rangle$	$\langle a+a,\beta,\gamma\rangle$	$\langle a+\beta,\gamma,\delta\rangle$	$\langle a,b,c\rangle$	$\langle\alpha+\alpha,\beta,\gamma\rangle$	$\langle a+b,c,d\rangle$
	$\langle\alpha+\gamma,\beta,\delta\rangle$	$\langle a+\beta,a,\gamma\rangle$	$\langle a+\gamma,\beta,\delta\rangle$	$\langle a,b,d\rangle$	$\langle\beta+\gamma,\alpha,\alpha\rangle$	$\langle a+c,b,d\rangle$
	$\langle\alpha+\delta,\beta,\gamma\rangle$	$\langle a+\beta,a,\gamma\rangle$	$\langle a+\delta,\beta,\gamma\rangle$	$\langle a,b,e\rangle$	$\langle\alpha+\beta,\alpha,\gamma\rangle$	$\langle a+d,b,c\rangle$
	$\langle\beta+\gamma,\alpha,\delta\rangle$	$\langle a+\gamma,a,\beta\rangle$	$\langle\beta+\gamma,a,\delta\rangle$	$\langle a,c,d\rangle$	$\langle\alpha+\beta,\alpha,\gamma\rangle$	$\langle b+c,a,d\rangle$
	$\langle\beta+\delta,\alpha,\gamma\rangle$	$\langle a+\gamma,a,\beta\rangle$	$\langle\beta+\delta,a,\gamma\rangle$	$\langle a,c,e\rangle$	$\langle\alpha+\gamma,\alpha,\beta\rangle$	$\langle b+d,a,c\rangle$
	$\langle\gamma+\delta,\alpha,\beta\rangle$	$\langle\beta+\gamma,a,a\rangle$	$\langle\gamma+\delta,a,\beta\rangle$	$\langle a,d,e\rangle$	$\langle\alpha+\gamma,\alpha,\beta\rangle$	$\langle c+d,a,b\rangle$

H	$\langle a,a,a,b,c,d\rangle$			$\langle a,a,b,b,c,c\rangle$		impossible configuration
type	IV.1	IV.2	IV.3	V.1	V.2	
M	$\langle a,a,a,\beta\rangle$	$\langle a,a,\beta,\gamma\rangle$	$\langle a,b,c,d\rangle$	$\langle\alpha,\alpha,\beta,\beta\rangle$	$\langle\alpha,\alpha,\beta,\gamma\rangle$	$\langle\alpha,\alpha,\beta,\beta\rangle$
E	$\langle\gamma,\delta\rangle$	$\langle a,\delta\rangle$	$\langle a,a\rangle$	$\langle\gamma,\gamma\rangle$	$\langle\beta,\gamma\rangle$	$\langle\gamma,\delta\rangle$
deck	$\langle a+a,a,\beta\rangle$	$\langle a+a,\beta,\gamma\rangle$	$\langle a,a,b\rangle$	$\langle\gamma,\alpha,\alpha\rangle$	$\langle\alpha+\alpha,\beta,\gamma\rangle$	$\langle\alpha+\alpha,\beta,\beta\rangle$
	$\langle a+a,a,\beta\rangle$	$\langle a+\beta,a,\gamma\rangle$	$\langle a,a,c\rangle$	$\langle\gamma,\beta,\beta\rangle$	$\langle\beta+\gamma,\alpha,\alpha\rangle$	$\langle\beta+\beta,\alpha,\alpha\rangle$
	$\langle a+a,a,\beta\rangle$	$\langle a+\beta,a,\gamma\rangle$	$\langle a,a,d\rangle$	$\langle\gamma,\alpha,\beta\rangle$	$\langle\alpha+\beta,\alpha,\gamma\rangle$	$\langle\alpha+\beta,\alpha,\beta\rangle$
	$\langle a+\beta,a,a\rangle$	$\langle a+\gamma,a,\beta\rangle$	$\langle a,b,c\rangle$	$\langle\gamma,\alpha,\beta\rangle$	$\langle\alpha+\beta,\alpha,\gamma\rangle$	$\langle\alpha+\beta,\alpha,\beta\rangle$
	$\langle a+\beta,a,a\rangle$	$\langle a+\gamma,a,\beta\rangle$	$\langle a,b,d\rangle$	$\langle\gamma,\alpha,\beta\rangle$	$\langle\alpha+\gamma,\alpha,\beta\rangle$	$\langle\alpha+\beta,\alpha,\beta\rangle$
	$\langle a+\beta,a,a\rangle$	$\langle\beta+\gamma,a,a\rangle$	$\langle a,c,d\rangle$	$\langle\gamma,\alpha,\beta\rangle$	$\langle\alpha+\gamma,\alpha,\beta\rangle$	$\langle\alpha+\beta,\alpha,\beta\rangle$

H	$\langle a,a,a,b,b,c\rangle$				$\langle a,a,a,a,b,c\rangle$	
type	VI.1	VI.2	VI.3	VI.4	VII.1	VII.2
M	$\langle a,a,a,b\rangle$	$\langle a,a,a,c\rangle$	$\langle a,a,b,c\rangle$	$\langle a,b,b,c\rangle$	$\langle a,a,a,\beta\rangle$	$\langle a,a,b,c\rangle$
E	$\langle b,c\rangle$	$\langle b,b\rangle$	$\langle a,b\rangle$	$\langle a,a\rangle$	$\langle a,\gamma\rangle$	$\langle a,a\rangle$
deck	$\langle a+a,a,b\rangle$	$\langle b,a,c\rangle$	$\langle a+a,b,c\rangle$	$\langle a,a,c\rangle$	$\langle a+a,a,\beta\rangle$	$\langle a,a,a\rangle$
	$\langle a+a,a,b\rangle$	$\langle b,a,c\rangle$	$\langle b+c,a,a\rangle$	$\langle a,b,b\rangle$	$\langle a+a,a,\beta\rangle$	$\langle a,b,c\rangle$
	$\langle a+a,a,b\rangle$	$\langle b,a,c\rangle$	$\langle a+b,a,c\rangle$	$\langle a,a,b\rangle$	$\langle a+a,a,\beta\rangle$	$\langle a,a,b\rangle$
	$\langle a+b,a,a\rangle$	$\langle b,a,a\rangle$	$\langle a+b,a,c\rangle$	$\langle a,a,b\rangle$	$\langle a+\beta,a,a\rangle$	$\langle a,a,b\rangle$
	$\langle a+b,a,a\rangle$	$\langle b,a,a\rangle$	$\langle a+c,a,b\rangle$	$\langle a,b,c\rangle$	$\langle a+\beta,a,a\rangle$	$\langle a,a,c\rangle$
	$\langle a+b,a,a\rangle$	$\langle b,a,a\rangle$	$\langle a+c,a,b\rangle$	$\langle a,b,c\rangle$	$\langle a+\beta,a,a\rangle$	$\langle a,a,c\rangle$

H	$\langle a,a,a,b,b,b\rangle$	$\langle a,a,a,a,b,b\rangle$			$\langle a,a,a,a,a,b\rangle$	$\langle a,a,a,a,a,a\rangle$
type	VIII.1	IX.1	IX.2	IX.3	X.1	XI.1
M	$\langle\alpha,\alpha,\alpha,\beta\rangle$	$\langle a,a,a,a\rangle$	$\langle a,a,a,b\rangle$	$\langle a,a,b,b\rangle$	$\langle a,a,a,b\rangle$	$\langle a,a,a,a\rangle$
E	$\langle\beta,\beta\rangle$	$\langle b,b\rangle$	$\langle a,b\rangle$	$\langle a,a\rangle$	$\langle a,a\rangle$	$\langle a,a\rangle$
deck	$\langle\beta,\alpha,\alpha\rangle$	$\langle b,a,a\rangle$	$\langle a+a,a,b\rangle$	$\langle a,a,a\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$
	$\langle\beta,\alpha,\alpha\rangle$	$\langle b,a,a\rangle$	$\langle a+a,a,b\rangle$	$\langle a,b,b\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$
	$\langle\beta,\alpha,\alpha\rangle$	$\langle b,a,a\rangle$	$\langle a+a,a,b\rangle$	$\langle a,a,b\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$
	$\langle\beta,\alpha,\beta\rangle$	$\langle b,a,a\rangle$	$\langle a+b,a,a\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$	$\langle a,a,a\rangle$
	$\langle\beta,\alpha,\beta\rangle$	$\langle b,a,a\rangle$	$\langle a+b,a,a\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$	$\langle a,a,a\rangle$
	$\langle\beta,\alpha,\beta\rangle$	$\langle b,a,a\rangle$	$\langle a+b,a,a\rangle$	$\langle a,a,b\rangle$	$\langle a,a,a\rangle$	$\langle a,a,a\rangle$

TABLE 1. The different types of multisets considered in the proof of Theorem 3.8.

form $X.Y$, where X is a Roman numeral and Y is an Arabic numeral. We will also write simply "M is of type $X.Y$" to mean "(M,E) is of type $X.Y$".

Before starting the case analysis, let us first rule out an impossible configuration that may arise as a $(4,2)$-partition of H. If $(M,E) = (\langle\alpha,\alpha,\beta,\beta\rangle, \langle\gamma,\delta\rangle)$ for some (not necessarily pairwise distinct) elements $\alpha,\beta,\gamma,\delta \in G$ such that $\gamma \neq \delta$, then $\langle\alpha+\beta,\alpha,\beta\rangle$ is a card of M with multiplicity 4 (if $\alpha \neq \beta$) or 6 (if $\alpha = \beta$). But then $\alpha+\beta$ should be equal to both γ and δ, a contradiction which shows that this case does not occur.

Case 1: $H = \langle a,b,c,d,e,f\rangle$ for some pairwise distinct elements $a,b,c,d,e,f \in G$. The $(4,2)$-partitions of H are of the form $(\langle\alpha,\beta,\gamma,\delta\rangle, \langle\epsilon,\zeta\rangle)$ (referred to as type

I.1), where $\{\alpha,\beta,\gamma,\delta,\epsilon,\zeta\} = \{a,b,c,d,e,f\}$. Thus, we may assume that $M = \langle\alpha,\beta,\gamma,\delta\rangle$, $E = \langle\epsilon,\zeta\rangle$, $M' = \langle\alpha',\beta',\gamma',\delta'\rangle$, $E' = \langle\epsilon',\zeta'\rangle$ with $\{\alpha,\beta,\gamma,\delta,\epsilon,\zeta\} = \{\alpha',\beta',\gamma',\delta',\epsilon',\zeta'\} = \{a,b,c,d,e,f\}$.

Suppose, on the contrary, that $M \neq M'$. Then $2 \leq |M \cap M'| \leq 3$. If $|M \cap M'| = 2$, then we may assume, without loss of generality, that $M' = \langle\alpha,\beta,\epsilon,\zeta\rangle$. Then $\alpha+\beta \in E \cap E' = \langle\epsilon,\zeta\rangle \cap \langle\gamma,\delta\rangle = \emptyset$, a contradiction. If $|M \cap M'| = 3$, then we may assume, without loss of generality, that $M' = \langle\alpha,\beta,\gamma,\epsilon\rangle$. Then $\alpha+\beta \in E \cap E' = \langle\epsilon,\zeta\rangle \cap \langle\delta,\zeta\rangle = \langle\zeta\rangle$; thus $\alpha+\beta = \zeta$. It follows that $\langle\zeta,\gamma,\epsilon\rangle$ is a card of M', but this cannot be a card of M, because ϵ and ζ do not occur together in any card of M. We have reached again a contradiction. We conclude that $M = M'$.

Case 2: $H = \langle a,a,b,c,d,e\rangle$ for some pairwise distinct elements $a,b,c,d,e \in G$. The $(4,2)$-partitions of H are the following: $(\langle a,a,\beta,\gamma\rangle, \langle\delta,\epsilon\rangle)$ (type II.1), $(\langle a,\beta,\gamma,\delta\rangle, \langle a,\epsilon\rangle)$ (type II.2), and $(\langle b,c,d,e\rangle, \langle a,a\rangle)$ (type II.3), where $\{\beta,\gamma,\delta,\epsilon\} = \{b,c,d,e\}$.

Consider first the case that M is of type II.1 and M' is of type II.2 or II.3. Then the deck of M has repeated cards while the cards of M' are all pairwise distinct; hence $\operatorname{deck} M \neq \operatorname{deck} M'$. We have reached a contradiction, which shows that this case is not possible.

Consider then the case that $M = \langle a,\beta,\gamma,\delta\rangle$ is of type II.2 and $M' = \langle b,c,d,e\rangle$ is of type II.3. Every card of M' contains exactly one occurrence of a. In order to have exactly one occurrence of a in every card of M, we must have $a+\beta = a+\gamma = a+\delta = a$; consequently $\beta+\gamma = \beta+\delta = \gamma+\delta = \epsilon$. The fact that M' is of type 2.C implies $x+y = a$ for all distinct $x,y \in \{b,c,d,e\}$. We have reached a contradiction, which shows that this case is not possible.

Consider then the case that $M = \langle a,a,\beta,\gamma\rangle$ and $M' = \langle a,a,\beta',\gamma'\rangle$ are both of type II.1, with $\{\beta,\gamma,\delta,\epsilon\} = \{\beta',\gamma',\delta',\epsilon'\} = \{b,c,d,e\}$. The only card of M with no occurrence of a is $\langle a+a,\beta,\gamma\rangle$, and the only card of M' with no occurrence of a is $\langle a+a,\beta',\gamma'\rangle$. These must be equal; hence $\{\beta,\gamma\} = \{\beta',\gamma'\}$, that is, $M = M'$.

Consider then the case that M and M' are both of type II.2. Suppose, on the contrary, that $M \neq M'$. We may assume, without loss of generality, that $M = \langle a,\beta,\gamma,\delta\rangle$, $M' = \langle a,\beta,\gamma,\epsilon\rangle$, where $\{\beta,\gamma,\delta,\epsilon\} = \{b,c,d,e\}$. Then $\beta+\gamma \in E \cap E' = \langle a,\epsilon\rangle \cap \langle a,\delta\rangle = \langle a\rangle$. Then $\langle a,a,\delta\rangle$ is a card of M, but this is not a card of M'. We have arrived in a contradiction, and we conclude that $M = M'$.

Finally, if M and M' are both of type II.3, then $M = M'$.

Case 3: $H = \langle a,a,b,b,c,d\rangle$ for some pairwise distinct elements $a,b,c,d \in G$. The possible $(4,2)$-partitions of H are the following: $(\langle\alpha,\alpha,\beta,\gamma\rangle, \langle\beta,\delta\rangle$ (type III.1) and $(\langle a,b,c,d\rangle, \langle a,b\rangle)$ (type III.2), where $\{\alpha,\beta\} = \{a,b\}$ and $\{\gamma,\delta\} = \{c,d\}$. (The $(4,2)$-partition $(\langle a,a,b,b\rangle, \langle c,d\rangle)$ of H is not possible, as noted above.)

Consider first the case that $M = \langle\alpha,\alpha,\beta,\gamma\rangle$ is of type III.1 and $M' = \langle a,b,c,d\rangle$ is of type III.2. Then $\alpha+\beta, \alpha+\gamma, \beta+\gamma \in E \cap E' = \langle\beta,\delta\rangle \cap \langle a,b\rangle = \langle\beta\rangle$, but then δ would appear only at most once in the cards of M. We have arrived in a contradiction, which shows that this case is not possible.

Consider then the case that $M = \langle\alpha,\alpha,\beta,\gamma\rangle$ and $M' = \langle\alpha',\alpha',\beta',\gamma'\rangle$ are both of type III.1, with $\{\alpha,\beta\} = \{\alpha',\beta'\} = \{a,b\}$, $\{\gamma,\delta\} = \{\gamma',\delta'\} = \{c,d\}$. If $\alpha' = \beta$ and $\gamma' = \delta$, then $\alpha+\beta = \alpha'+\beta' \in E \cap E' = \langle\beta,\delta\rangle \cap \langle\alpha,\gamma\rangle = \emptyset$, a contradiction. If $\alpha' = \alpha$ and $\gamma' = \delta$, then $\alpha+\alpha, \alpha+\beta \in E \cap E' = \langle\beta,\delta\rangle \cap \langle\beta,\gamma\rangle = \langle\beta\rangle$; consequently, $\langle\beta,\beta,\gamma\rangle$ is a card of M but not a card of M', a contradiction. If $\alpha' = \beta$ and $\gamma' = \gamma$, then $\alpha+\beta, \beta+\gamma \in E \cap E' = \langle\beta,\delta\rangle \cap \langle\alpha,\delta\rangle = \langle\delta\rangle$; but then δ will occur at least

4 times in the cards of M', a contradiction. We are left with the case that $\alpha' = \alpha$ and $\gamma' = \gamma$, that is, $M = M'$.

Finally, if M and M' are both of the form III.2, then $M = M'$.

Case 4: $H = \langle a, a, a, b, c, d\rangle$ for some pairwise distinct elements $a, b, c, d \in G$. The $(4, 2)$-partitions of H are the following: $(\langle a, a, a, \beta\rangle, \langle \gamma, \delta\rangle)$ (type IV.1), $(\langle a, a, \beta, \gamma\rangle, \langle a, \delta\rangle)$ (type IV.2), and $(\langle a, b, c, d\rangle, \langle a, a\rangle)$ (type IV.3), where $\{\beta, \gamma, \delta\} = \{b, c, d\}$.

Consider first the case that M is of type IV.1 or IV.2 and M' is of type IV.3. Then M has repeated cards while the cards of M' are pairwise distinct; hence $\operatorname{deck} M \neq \operatorname{deck} M$. We have reached a contradiction, which shows that this case is not possible.

Consider then the case that $M = \langle a, a, a, \beta\rangle$ is of type IV.1 and $M' = \langle a, a, \beta', \gamma'\rangle$ is of type IV.2, with $\{\beta, \gamma, \delta\} = \{\beta', \gamma', \delta'\} = \{b, c, d\}$. If $\{\beta\} \cap \{\beta', \gamma'\} = \emptyset$, then actually $\{\beta', \gamma'\} = \{\gamma, \delta\}$ and $\delta' = \beta$. Then we would have $a + a \in E \cap E' = \langle \gamma, \delta\rangle \cap \langle a, \beta\rangle = \emptyset$, a contradiction. Thus, we may assume that $\beta \in \{\beta', \gamma'\}$. Then we have that $a + a, a + \beta \in E \cap E' \langle \gamma, \delta\rangle \cap \langle a, \delta'\rangle = \langle \delta'\rangle$. On the other hand, it follows from the fact that M is of type IV.1 that $a + a \neq a + \beta$. We have reached again a contradiction, and we conclude that this case is not possible.

Consider then the case that $M = \langle a, a, a, \beta\rangle$ and $M' = \langle a, a, a, \beta'\rangle$ are both of type IV.1, with $\{\beta, \gamma, \delta\} = \{\beta', \gamma', \delta'\} = \{b, c, d\}$. Since $a + a \in E \cap E' = \langle \gamma, \delta\rangle \cap \langle \gamma', \delta'\rangle$, we have that $a + a \neq a$. Therefore, the only cards of M with a single occurrence of a are the three copies of $\langle a + a, a, \beta\rangle$, and the only cards of M' with a single occurrence of a are the three copies of $\langle a + a, a, \beta'\rangle$. This implies that $\beta = \beta'$; hence $M = M'$.

Consider then the case that $M = \langle a, a, \beta, \gamma\rangle$ and $M' = \langle a, a, \beta', \gamma'\rangle$ are both of type IV.2, with $\{\beta, \gamma, \delta\} = \{\beta', \gamma', \delta'\} = \{b, c, d\}$. Suppose, on the contrary, that $M \neq M'$. We may assume, without loss of generality, that $\beta = \beta'$ and $\gamma' = \delta$. Then $a + a, a + \beta \in E \cap E' = \langle a, \delta\rangle \cap \langle a, \gamma\rangle = \langle a\rangle$. Consequently, $\langle a, \beta, \gamma\rangle$ has multiplicity exactly 1 in the deck of M but it has multiplicity 2 in the deck of M', a contradiction. We conclude that $M = M'$.

Finally, if M and M' are both of type IV.3, then $M = M'$.

Case 5: $H = \langle a, a, b, b, c, c\rangle$ for some pairwise distinct elements $a, b, c \in G$. The $(4, 2)$-partitions of H are the following: $(\langle \alpha, \alpha, \beta, \beta\rangle, \langle \gamma, \gamma\rangle)$ (type V.1) and $(\langle \alpha, \alpha, \beta, \gamma\rangle, \langle \beta, \gamma\rangle)$ (type V.2), where $\{\alpha, \beta, \gamma\} = \{a, b, c\}$.

Consider first the case that $M = \langle \alpha, \alpha, \beta, \beta\rangle$ is of type V.1 and $M' = \langle \alpha', \alpha', \beta', \gamma'\rangle$ is of type V.2, with $\{\alpha, \beta, \gamma\} = \{\alpha', \beta', \gamma'\} = \{a, b, c\}$. The element γ occurs exactly once in every card of M. One of the cards of M', namely $\langle \beta' + \gamma', \alpha', \alpha'\rangle$, has two occurrences of α'; hence $\alpha' \neq \gamma$. Suppose $\beta' = \gamma$; in other words, $\{\alpha', \gamma'\} = \{\alpha, \beta\}$. Then we must have $\beta' + \gamma' = \alpha' + \beta' = \gamma = \beta'$; consequently, $\alpha' + \alpha' = \alpha' + \gamma' = \gamma' \neq \gamma$, but this contradicts the fact that $\alpha + \alpha = \alpha + \beta = \beta + \beta = \gamma$, implied by the fact that M is of type V.1. Thus, we remain with the possibility that $\gamma' = \gamma$; in other words, $\{\alpha', \beta'\} = \{\alpha, \beta\}$. Then $\beta' + \gamma' = \alpha' + \gamma' = \gamma = \gamma'$; consequently, $\alpha' + \alpha' = \alpha' + \beta' = \beta' \neq \gamma$, and we arrive similarly in a contradiction. We conclude that this case is not possible.

Consider then the case that $M = \langle \alpha, \alpha, \beta, \beta\rangle$ and $M' = \langle \alpha', \alpha', \beta', \beta'\rangle$ are both of type V.1, with $\{\alpha, \beta, \gamma\} = \{\alpha', \beta', \gamma'\} = \{a, b, c\}$. Then the unique element occurring exactly once in every card of M is γ, and the unique element occurring exactly once in every card of M' is γ'. Hence $\gamma = \gamma'$, that is, $M = M'$.

Consider finally the case that $M = \langle \alpha, \alpha, \beta, \gamma \rangle$ and $M' = \langle \alpha', \alpha', \beta', \gamma' \rangle$ are both of type V.2, with $\{\alpha, \beta, \gamma\} = \{\alpha', \beta', \gamma'\} = \{a, b, c\}$. Suppose, on the contrary, that $M \neq M'$. We may assume, without loss of generality, that $M' = \langle \beta, \beta, \alpha, \gamma \rangle$. Then we have that $\alpha + \beta, \alpha + \gamma \in E \cap E' = \langle \beta, \gamma \rangle \cap \langle \alpha, \gamma \rangle = \langle \gamma \rangle$, and we will have too many γ's occurring in the cards of M, a contradiction. We conclude that $M = M'$.

Case 6: $H = \langle a, a, a, b, b, c \rangle$ for some pairwise distinct elements $a, b, c \in G$. The possible $(4, 2)$-partitions of H are the following: $(\langle a, a, a, b \rangle, \langle b, c \rangle)$ (type VI.1), $(\langle a, a, a, c \rangle, \langle b, b \rangle)$ (type VI.2), $(\langle a, a, b, c \rangle, \langle a, b \rangle)$ (type VI.3), and $(\langle a, b, b, c \rangle, \langle a, a \rangle)$ (type VI.4). (The $(4, 2)$-partition $(\langle a, a, b, b \rangle, \langle a, c \rangle)$ of H is not possible, as noted above.)

If M and M' are of the same type, VI.1, VI.2, VI.3, or VI.4, then clearly $M = M'$. Suppose then, on the contrary, that M and M' are of different types.

Assume that M is of type VI.4. Then $a + b = a + c = b + c = b + b = a$. If M' is of type VI.1, then $a + b \neq a$, a contradiction. If M' is of type VI.2, then $a + a = a + c = b$, a contradiction. If M' is of type VI.3, then $a + b$ and $a + c$ are not both equal to a, a contradiction.

Assume that M is of type VI.2. Then $a + a = b$. If M' is of type VI.1, then $\langle b, a, b \rangle$ is a card of M' but it is not a card of M, a contradiction. If M' is of type VI.3, then $\langle b, b, c \rangle$ is a card of M' but it is not a card of M, a contradiction.

Assume that M is of type VI.1 and M' is of type VI.3. The fact that M is of type VI.1 implies $\{a + a, a + b\} = \{b, c\}$. The fact that M' is of type VI.3 implies $\{a + a, a + b\} \subseteq \{a, b\}$, a contradiction.

Case 7: $H = \langle a, a, a, a, b, c \rangle$ for some pairwise distinct elements $a, b, c \in G$. The possible $(4, 2)$-partitions of H are the following: $(\langle a, a, a, \beta \rangle, \langle a, \gamma \rangle)$ (type VII.1) and $(\langle a, a, b, c \rangle, \langle a, a \rangle)$ (type VII.2), where $\{\beta, \gamma\} = \{b, c\}$. (The $(4, 2)$-partition $(\langle a, a, a, a \rangle, \langle b, c \rangle)$ of G is not possible, as noted above.)

Consider first the case that M is of type VII.1 and M' is of type VII.2. Then $\langle a, a, a \rangle$ has multiplicity 1 in the deck of M', but its multiplicity is either 0 or 3 in the deck of M, a contradiction. We conclude that this case is not possible.

Consider then the case that M and M' are both of type VII.1. If $M = M'$, then we are done. Assume that $M \neq M$. We may assume that $M = \langle a, a, a, b \rangle$ and $M' = \langle a, a, a, c \rangle$. Then $a + a \in E \cap E' = \langle a, c \rangle \cap \langle a, b \rangle = \langle a \rangle$. This implies that $a + b = c$ and $a + c = b$. Choosing $r := a$, $s := a$, $t := a$, $u := b$, $v := c$, we see that condition (ii) holds.

Finally, if M and M' are both of type VII.2, then $M = M'$.

Case 8: $H = \langle a, a, a, b, b, b \rangle$ for some distinct elements $a, b \in G$. The $(4, 2)$-partitions of H are of the form $(\langle \alpha, \alpha, \alpha, \beta \rangle, \langle \beta, \beta \rangle)$ (type VIII.1), where $\{\alpha, \beta\} = \{a, b\}$. (The $(4, 2)$-partition $(\langle a, a, b, b \rangle, \langle a, b \rangle)$ of G is not possible, as noted above.)

Suppose, on the contrary, that $M \neq M'$. We may assume that $M = \langle a, a, a, b \rangle$ and $M' = \langle b, b, b, a \rangle$. Then $a + a = a + b = b$ and $b + b = b + a = a$, a contradiction. We conclude that $M = M'$.

Case 9: $H = \langle a, a, a, a, b, b \rangle$ for some distinct elements $a, b \in G$. The $(4, 2)$-partitions of H are the following: $(\langle a, a, a, a \rangle, \langle b, b \rangle)$ (type IX.1), $(\langle a, a, a, b \rangle, \langle a, b \rangle)$ (type IX.2), and $(\langle a, a, b, b \rangle, \langle a, a \rangle)$ (type IX.3).

If M and M' are of the same type, IX.1, IX.2, or IX.3, then clearly $M = M'$. Suppose, on the contrary, that M and M' are of different types.

Assume that M is of type IX.1. Then $a + a = b$. If M' is of type IX.2, then $\langle b, a, b\rangle$ is a card of M', but this is not a card of M, a contradiction. If M' is of type IX.3, then $a + a = a$, a contradiction.

Assume that M is of type IX.2. Then $a + a \neq a + b$. If M' is of type IX.3, then $a + a = a + b = b + b = a$, a contradiction.

Case 10: $H = \langle a, a, a, a, a, b\rangle$ for some distinct elements $a, b \in G$. The only possible $(4, 2)$-partition of H is $(\langle a, a, a, b\rangle, \langle a, a\rangle)$ (type X.1). (The $(4, 2)$-partition $(\langle a, a, a, a\rangle, \langle a, b\rangle)$ of H is not possible, as noted above.) Therefore, $M = M'$.

Case 11: $H = \langle a, a, a, a, a, a\rangle$ for some $a \in G$. The only $(4, 2)$-partition of H is $(\langle a, a, a, a\rangle, \langle a, a\rangle)$ (type XI.1), and it holds that $M = M'$.

We have exhausted all possible cases, and have arrived at the desired conclusion. This completes the proof of the theorem. □

Theorem 3.9. *Assume that $(G; +)$ is a commutative groupoid. Let M and M' be multisets of cardinality 3 over G. Then* $\operatorname{deck} M = \operatorname{deck} M'$ *if and only if one of the following conditions holds:*

(i) $M = M'$.
(ii) $M = \langle r, s, t\rangle$, $M' = \langle r, r + s, r + t\rangle$ *for some elements* $r, s, t \in G$ *satisfying* $r + (r + s) = s$, $r + (r + t) = t$, $(r + s) + (r + t) = s + t$.
(iii) $M = \langle r, s, t\rangle$, $M' = \langle r + s, r + t, s + t\rangle$ *for some elements* $r, s, t \in G$ *satisfying* $(r + s) + (r + t) = r$, $(r + s) + (s + t) = s$, $(r + t) + (s + t) = t$.

Proof. It is clear that if $M = M'$, then $\operatorname{deck} M = \operatorname{deck} M'$. If condition (ii) or (iii) holds, then $\operatorname{deck} M = \operatorname{deck} M'$, as shown in Examples 3.2 and 3.3.

For the converse implication, assume that $\operatorname{deck} M = \operatorname{deck} M'$. Assume that $M = \langle a, b, c\rangle$ and $M' = \langle \alpha, \beta, \gamma\rangle$. Then

$$\operatorname{deck} M = \langle\langle a, b + c\rangle, \langle b, a + c\rangle, \langle c, a + b\rangle\rangle,$$
$$\operatorname{deck} M' = \langle\langle \alpha, \beta + \gamma\rangle, \langle \beta, \alpha + \gamma\rangle, \langle \gamma, \alpha + \beta\rangle\rangle.$$

Relabeling the elements of M' if necessary, we may assume that

$$\langle \alpha, \beta + \gamma\rangle = \langle a, b + c\rangle, \quad \langle \beta, \alpha + \gamma\rangle = \langle b, a + c\rangle, \quad \langle \gamma, \alpha + \beta\rangle = \langle c, a + b\rangle.$$

If $(\alpha, \beta + \gamma) = (a, b + c)$, $(\beta, \alpha + \gamma) = (b, a + c)$, $(\gamma, \alpha + \beta) = (c, a + b)$, then $M = M'$ and we are done.

If $(\alpha, \beta + \gamma) = (a, b + c)$, $(\beta, \alpha + \gamma) = (b, a + c)$, $(\gamma, \alpha + \beta) = (a + b, c)$, then we have $c = \alpha + \beta = a + b = \gamma$. Hence $M = M'$ and we are done. If $(\alpha, \beta + \gamma) = (a, b + c)$, $(\beta, \alpha + \gamma) = (a + c, b)$, $(\gamma, \alpha + \beta) = (c, a + b)$ or $(\alpha, \beta + \gamma) = (b + c, a)$, $(\beta, \alpha + \gamma) = (b, a + c)$, $(\gamma, \alpha + \beta) = (c, a + b)$, then a similar argument shows that $M = M'$ and we are done.

If $(\alpha, \beta + \gamma) = (a, b + c)$, $(\beta, \alpha + \gamma) = (a + c, b)$, $(\gamma, \alpha + \beta) = (a + b, c)$, then $a + (a + b) = \alpha + \gamma = b$, $a + (a + c) = \alpha + \beta = c$ and $(a + b) + (a + c) = \gamma + \beta = b + c$. Choosing $r := a$, $s := b$, $t := c$, we see that condition (ii) holds and we are done. We argue similarly in the case when $(\alpha, \beta + \gamma) = (b + c, a)$, $(\beta, \alpha + \gamma) = (b, a + c)$, $(\gamma, \alpha + \beta) = (a + b, c)$ or $(\alpha, \beta + \gamma) = (b + c, a)$, $(\beta, \alpha + \gamma) = (a + c, b)$, $(\gamma, \alpha + \beta) = (c, a + b)$ to show that condition (ii) holds.

We are left with the case that $(\alpha, \beta + \gamma) = (b + c, a)$, $(\beta, \alpha + \gamma) = (a + c, b)$, $(\gamma, \alpha + \beta) = (a + b, c)$. Then $(a + b) + (a + c) = \gamma + \beta = a$, $(a + b) + (b + c) = \gamma + \alpha = b$ and $(a + c) + (b + c) = \beta + \alpha = c$. Choosing $r := a$, $s := b$, $t := c$, we see that condition (iii) holds. □

Theorem 3.10. *Assume that $(G;+)$ is a commutative groupoid. Let M and M' be multisets of cardinality 2 over G. Then* $\operatorname{deck} M = \operatorname{deck} M'$ *if and only if $M = \langle r, s\rangle$, $M' = \langle t, u\rangle$ for some elements $r, s, t, u \in G$ such that $r + s = t + u$.*

Proof. Obvious. □

Remark 3.11. Let $(G;+)$ be a commutative groupoid. Every multiset of cardinality 2 over G is reconstructible if and only if for all $a, b, c, d \in G$, it holds that

$$a + b = c + d \iff (a, b) = (c, d) \text{ or } (a, b) = (d, c).$$

Examples of groupoids satisfying this condition include the free commutative groupoids (see the paper by Prešić [11]).

3.3. **Open problems.** We have completely solved the reconstruction problem for multisets over commutative groupoids. We conclude this section by suggesting some possible directions for future research. A common variant of reconstruction problems is the so-called set reconstruction problem: we define deck as a *set* of cards instead of a *multiset* of cards and then ask whether an object is uniquely determined (up to isomorphism) by its set of cards. The set reconstruction problem for multisets over commutative groupoids is an open problem, and it may be worth investigating.

Another related question is the following: Is reconstruction possible from a few cards only? More precisely, for a commutative groupoid $(G;+)$ and an integer $n \geq 2$, what is the smallest number m such that every multiset M of cardinality n over G is uniquely determined by any m of its cards? This remains an open problem, but let us make a few simple observations. This number may be as large as $\binom{n}{2}$, i.e., all cards are needed for reconstruction, as the following example illustrates.

Example 3.12. Let $(G;+)$ be the 2-element group of addition modulo 2, and let $n = 4$. Let $M = \langle 1, 1, 1, 1\rangle$, $M' = \langle 0, 0, 1, 1\rangle$. Then

$$\operatorname{deck} M = \langle \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle\rangle,$$
$$\operatorname{deck} M = \langle \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 0, 0\rangle\rangle.$$

Even though every 4-multiset over G is reconstructible by Theorem 3.8, M and M' cannot be reconstructed from 5 cards only: the decks of both M and M' include 5 copies of $\langle 0, 1, 1\rangle$.

If $(G;+)$ is a commutative group, then 2 cards do not suffice for reconstruction. This clearly holds for 2-multisets, and the following example shows that this is also the case for multisets of cardinality at least 3.

Example 3.13. Let $(G;+)$ be a commutative group and assume that $n \geq 3$. Let $M = \langle m_1, \ldots, m_n\rangle$, $M' = \langle m_1 + m_2, m_2 + m_3, -m_2, m_4, \ldots, m_n\rangle$. Then

$$\langle m_1 + m_2, m_3, m_4, \ldots, m_n\rangle \quad \text{and} \quad \langle m_1, m_2 + m_3, m_4, \ldots, m_n\rangle$$

are cards of both M and M'.

4. Reconstruction problem for functions of several arguments – the case of affine functions

As mentioned in the introduction, the reconstruction problem for multisets over commutative groupoids arose from a completely different reconstruction problem

formulated for functions of several arguments. In the special case of affine functions over nonassociative semirings, the reconstruction problem for functions reduces to the reconstruction problem for multisets over commutative groupoids. In this section, we will apply our results on the reconstructibility of multisets to the reconstruction problem for functions.

4.1. **Functions of several arguments and identification minors.** Let A and B be arbitrary sets with at least two elements. A *function* (*of several arguments*) from A to B is a map $f\colon A^n \to B$ for some positive integer n, called the *arity* of f. Functions of several arguments from A to A are called *operations* on A. We denote the set of all n-ary functions from A to B by $\mathcal{F}_{AB}^{(n)}$, and we denote the set of all functions from A to B of any finite arity by $\mathcal{F}_{AB}$; in other words, $\mathcal{F}_{AB}^{(n)} = B^{A^n}$ and $\mathcal{F}_{AB} = \bigcup_{n\geq 1} \mathcal{F}_{AB}^{(n)}$. For $1 \leq i \leq n$, the i-th n-ary *projection* on A is the operation $(a_1, \dots, a_n) \mapsto a_i$ for all $(a_1, \dots, a_n) \in A^n$.

Let $f\colon A^n \to B$. For $i \in [n]$, the i-th argument of f is *essential,* or f *depends* on the i-th argument, if there exist tuples $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A^n$ such that $a_j = b_j$ for all $j \in [n] \setminus \{i\}$ and $f(a_1, \dots, a_n) \neq f(b_1, \dots, b_n)$.

Two functions $f, g\colon A^n \to B$ are *equivalent*, denoted $f \equiv g$, if there exists a bijection $\sigma\colon [n] \to [n]$ such that $f(a_1, \dots, a_n) = g(a_{\sigma(1)}, \dots, a_{\sigma(n)})$ for all $(a_1, \dots, a_n) \in A^n$.

Let $n \geq 2$, and let $f\colon A^n \to B$. For each $I \in \binom{n}{2}$, we define the function $f_I\colon A^{n-1} \to B$ by the rule

$$f_I(a_1, \dots, a_{n-1}) = f(a_1, \dots, a_{\max I - 1}, a_{\min I}, a_{\max I}, \dots, a_{n-1}).$$

Note that $a_{\min I}$ occurs twice on the right side of the above equality, namely, at the two positions indexed by the elements of I. We will refer to the function f_I as an *identification minor* of f. This name is motivated by the fact that f_I is obtained from f by identifying the arguments indexed by the couple I.

Lemma 4.1 (Willard [14, Lemma 1.2])**.** *Let A and B nonempty sets, and let $f\colon A^n \to B$. Assume that f depends on all of its arguments. If $n > |A|$, then there exists $I \in \binom{n}{2}$ such that f_I depends on at least $n-2$ arguments.*

4.2. **Reconstruction problem for functions of several arguments.** Assume that $n \geq 2$ and let $f\colon A^n \to B$. The *deck* of f, denoted $\operatorname{deck} f$, is the multiset $\langle f_I/{\equiv} : I \in \binom{n}{2}\rangle$ of the equivalence classes of the identification minors of f. Any element of the deck of f is called a *card* of f. A function $g\colon A^n \to B$ is a *reconstruction* of f, if $\operatorname{deck} f = \operatorname{deck} g$. A function is *reconstructible* if it is equivalent to all of its reconstructions. A class $\mathcal{C} \subseteq \mathcal{F}_{AB}$ of functions is *reconstructible* if all members of $\mathcal{C}$ are reconstructible. A class $\mathcal{C} \subseteq \mathcal{F}_{AB}$ is *weakly reconstructible* if for every $f \in \mathcal{C}$, all reconstructions of f that are members of $\mathcal{C}$ are equivalent to f. A class $\mathcal{C} \subseteq \mathcal{F}_{AB}$ is *recognizable* if all reconstructions of the members of $\mathcal{C}$ are members of $\mathcal{C}$. Note that if a class of functions is recognizable and weakly reconstructible, then it is reconstructible.

This reconstruction problem was formulated and some results, both positive and negative, on the reconstructibility of functions were presented in [7]. The reader is referred to this paper for more details, motivations and background information.

4.3. **On the reconstructibility of affine functions.** By a *nonassociative right semiring* we mean an algebra $(G;+,\cdot)$ with binary operations $+$ and $\cdot$ called *addition* and *multiplication*, respectively, such that

- $(G;+)$ is a commutative monoid with neutral element 0 ($0+a=a+0=a$),
- $(G;\cdot)$ is a groupoid with right identity 1 ($a\cdot 1=a$),
- multiplication right distributes over addition ($(a+b)\cdot c=a\cdot c+b\cdot c$),
- multiplication on the right by 0 annihilates G ($a\cdot 0=0$).

A nonassociative right semiring $(G;+,\cdot)$ is *cancellative* if the additive monoid $(G;+)$ is cancellative, i.e., $a+b=a+c$ implies $b=c$. We will denote multiplication simply be concatenation.

The attribute "nonassociative" refers to the fact that we do not require that multiplication be associative, contrary to the usual practice with semirings. The attribute "right" refers to the fact that we only stipulate right multiplicative identity, right distributivity, and right annihilation. A *nonassociative left semiring* could be defined analogously, but we will not need this notion here. Examples of nonassociative right semirings include semirings, rings, fields, and bounded distributive lattices. Rings and fields are cancellative.

A function $f\colon G^n\to G$ is *affine* over $(G;+,\cdot)$ if

$$f(x_1,\dots,x_n)=a_1x_1+\cdots+a_nx_n+c, \tag{1}$$

for some $a_1,\dots,a_n,c\in G$. If $c=0$, then f is *linear*.

Lemma 4.2. *Let $(G;+,\cdot)$ be a nonassociative right semiring. Let f be an affine function over $(G;+,\cdot)$. If f is linear or if $(G;+,\cdot)$ is cancellative, then f has a unique representation of the form* (1).

Proof. Let $f\colon G^n\to G$, $f(x_1,\dots,x_n)=a_1x_1+\cdots+a_nx_n+c$. Assume that $f(x_1,\dots,x_n)=a'_1x_1+\cdots+a'_nx_n+c'$ for some $a'_1,\dots,a'_n,c'\in G$. Then $c=f(0,\dots,0)=c'$, and for every $i\in[n]$, $a_i+c=f(\mathbf{e}_i)=a'_i+c'=a'_i+c$, where $\mathbf{e}_i$ denotes the n-tuple in which the i-th entry is 1 and the remaining entries are 0. If f is linear (i.e., $c=0$) or if $(G;+,\cdot)$ is cancellative, then $a_i=a'_i$ for all $i\in[n]$. □

Let $f(x_1,\dots,x_n)=a_1x_1+\cdots+a_nx_n+c$. Denote by C_f the multiset $\langle a_1,\dots,a_n\rangle$ of the coefficients of the non-constant terms of f.

Lemma 4.3. *Let $(G;+,\cdot)$ be a nonassociative right semiring. Let $f,g\colon G^n\to G$ be affine functions over $(G;+,\cdot)$. Assume that f and g are linear or $(G;+,\cdot)$ is cancellative. Then $f\equiv g$ if and only if $C_f=C_g$ and the constant terms of f and g are equal.*

Proof. Let $f(x_1,\dots,x_n)=\sum_{i=1}^n a_ix_i+c$ and $g(x_1,\dots,x_n)=\sum_{i=1}^n b_ix_i+d$. Assume first that $f\equiv g$. Then there exists a permutation $\sigma\colon[n]\to[n]$ such that $f(a_1,\dots,a_n)=g(a_{\sigma(1)},\dots,a_{\sigma(n)})$ for all $(a_1,\dots,a_n)\in G^n$. Thus, $f(x_1,\dots,x_n)=\sum_{i=1}^n b_ix_{\sigma(i)}+d$. By Lemma 4.2, $c=d$ and $a_i=b_{\sigma^{-1}(i)}$ for all $i\in[n]$. Thus, $C_f=\langle a_1,\dots,a_n\rangle=\langle b_{\sigma^{-1}(1)},\dots,b_{\sigma^{-1}(n)}\rangle=C_g$.

For the converse implication, assume that $c=d$ and $C_f=C_g$. Then there exists a permutation $\sigma\colon[n]\to[n]$ such that $a_i=b_{\sigma(i)}$ for all $i\in[n]$. We have

$$\begin{aligned}f(x_1,\dots,x_n)&=a_1x_1+\cdots+a_nx_n+c=b_{\sigma(1)}x_1+\cdots+b_{\sigma(n)}x_n+d\\&=b_1x_{\sigma^{-1}(1)}+\cdots+b_nx_{\sigma^{-1}(n)}+d=g(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)}).\end{aligned}$$

Thus $f\equiv g$. □

For a multiset M over G and $c \in G$, with $|M| = n$, denote by $F_{M,c}$ the set $\{f\colon G^n \to G : C_f = M,\ f(0,\dots,0) = c\}$. It is clear from the definition and from Lemma 4.3 that $F_{M,c} = F_{M',c'}$ if and only if $M = M'$ and $c = c'$.

Lemma 4.4. *Let $f\colon G^n \to G$ be an affine function over a nonassociative right semiring $(G;+,\cdot)$. Then $\operatorname{deck} C_f = \langle C_{f_I} : I \in \binom{n}{2}\rangle$ and $\operatorname{deck} f = \langle F_{M_I,c} : I \in \binom{n}{2}\rangle$, where $c = f(0,\dots,0)$ and $(M_I)_{I\in\binom{n}{2}}$ is an indexed family satisfying $\operatorname{deck} C_f = \langle M_I : I \in \binom{n}{2}\rangle$.*

Proof. Let $f(x_1,\dots,x_n) = a_1x_1 + \cdots + a_nx_n + c$. Then $C_f = \langle a_1,\dots,a_n\rangle$ and $c = f(0,\dots 0)$. For each $I \in \binom{n}{2}$, let $(C_f)_I := C_f \setminus \langle a_{\min I}, a_{\max I}\rangle \uplus \langle a_{\min I} + a_{\max I}\rangle$. Then $\operatorname{deck} C_f = \langle (C_f)_I : I \in \binom{n}{2}\rangle$. For each $I \in \binom{n}{2}$,

$$f_I(x_1,\dots,x_{n-1}) = (a_{\min I} + a_{\max I})x_{\min I} + \sum_{i=1}^{\min I-1} a_ix_i + \sum_{i=\min I+1}^{\max I-1} a_ix_i + \sum_{i=\max I+1}^{n} a_ix_{i-1}.$$

Thus $C_{f_I} = (C_f)_I$. We conclude that $\operatorname{deck} C_f = \langle (C_f)_I : I \in \binom{n}{2}\rangle = \langle C_{f_I} : I \in \binom{n}{2}\rangle$ and $\operatorname{deck} f = \langle f_I/{\equiv} : I \in \binom{n}{2}\rangle = \langle F_{C_{f_I},c} : I \in \binom{n}{2}\rangle = \langle F_{(C_f)_I,c} : I \in \binom{n}{2}\rangle$. □

Theorem 4.5. *Let $f, g\colon G^n \to G$ be affine functions over a nonassociative right semiring $(G;+,\cdot)$ with $n \geq 4$. If f and g are linear or if $(G;+,\cdot)$ is cancellative, then $\operatorname{deck} f = \operatorname{deck} g$ if and only if $f \equiv g$.*

Proof. Let

$$f(x_1,\dots,x_n) = a_1x_1 + \cdots + a_nx_n + c,$$
$$g(x_1,\dots,x_n) = b_1x_1 + \cdots + b_nx_n + d,$$

for some $a_1,\dots,a_n,b_1,\dots,b_n,c,d \in G$. We assume that $c = d = 0$ or $(G;+,\cdot)$ is cancellative.

It is clear that if $f \equiv g$ then $\operatorname{deck} f = \operatorname{deck} g$. Assume that $\operatorname{deck} f = \operatorname{deck} g$. Since $f_I(0,\dots,0) = f(0,\dots,0) = c$ and $g_I(0,\dots,0) = g(0,\dots 0) = d$ for all $I \in \binom{n}{2}$, we must have that $c = d$.

By Lemma 4.4, $\operatorname{deck} f = \langle F_{M_I,c} : I \in \binom{n}{2}\rangle$ and $\operatorname{deck} g = \langle F_{M'_I,c} : I \in \binom{n}{2}\rangle$, where $(M_I)_{I\in\binom{n}{2}}$ and $(M'_I)_{I\in\binom{n}{2}}$ are indexed families satisfying $\langle M_I : I \in \binom{n}{2}\rangle = \operatorname{deck} C_f$ and $\langle M'_I : I \in \binom{n}{2}\rangle = \operatorname{deck} C_g$. Since $F_{M,c} = F_{M',c}$ if and only if $M = M'$, we have that $\operatorname{deck} C_f = \operatorname{deck} C_g$. If $n \geq 5$, then Theorem 3.7 implies that $C_f = C_g$. Since $(G;+)$ is associative, Theorem 3.8 implies, in light of Example 3.1, that $C_f = C_g$ in the case that $n = 4$. Applying Lemma 4.3, we conclude that $f \equiv g$. □

Theorem 4.5 asserts that the class of linear functions of arity at least 4 over any nonassociative right semiring $(G;+,\cdot)$ is weakly reconstructible. Furthermore, if $(G;+,\cdot)$ is cancellative, then the class of affine functions of arity at least 4 over $(G;+,\cdot)$ is weakly reconstructible.

Let us consider the special case when $(G,+,\cdot)$ is a finite field of order $q = p^k$ (p prime). It is well known that every operation on a finite field is a polynomial function. Moreover, each function $f\colon G^n \to G$ is induced by a unique polynomial in n variables where every exponent of every occurrence of every variable is at most $q-1$. Such a polynomial is referred to as the *canonical polynomial* of f. It is easy

to verify that a polynomial function f depends on the i-th argument if and only if the variable x_i occurs in the canonical polynomial of f.

Lemma 4.6. *Assume that $(G;+,\cdot)$ is a finite field of order $q = p^k$. If $n > \max(q,3)$ and $f\colon G^n \to G$ is not affine, then there exists $I \in \binom{n}{2}$ such that f_I is not affine.*

Proof. The canonical polynomial of f can be written as $P = \sum_{\mathbf{r}\in\{0,\dots,q-1\}^n} a_{\mathbf{r}}\mathbf{x}^{\mathbf{r}}$, where $\mathbf{r} = (r_1,\dots,r_n)$ and $\mathbf{x}^{\mathbf{r}} = x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$. Let P_{aff} be the polynomial comprising the monomials of P of total degree at most 1, and let P_{non} be the polynomial comprising the monomials of P_g of total degree at least 2, i.e.,

$$P_{\mathrm{aff}} = a_{\mathbf{0}} + \sum_{i=1}^{n} a_{\mathbf{e}_i} x_i, \qquad P_{\mathrm{non}} = \sum_{\mathbf{r}\in\{0,\dots,q-1\}^n\setminus\{\mathbf{0},\mathbf{e}_1,\dots,\mathbf{e}_n\}} a_{\mathbf{r}}\mathbf{x}^{\mathbf{r}},$$

where $\mathbf{0} = (0,\dots,0)$ and $\mathbf{e}_i$ is the n-tuple in which the i-th entry is 1 and the remaining entries are 0. Let $f_{\mathrm{aff}}, f_{\mathrm{non}}\colon G^n \to G$ be the functions induced by the polynomials P_{agg} and P_{non}, respectively. Then clearly $P = P_{\mathrm{aff}} + P_{\mathrm{non}}$ and $f = f_{\mathrm{aff}} + f_{\mathrm{non}}$ (pointwise addition of functions). Furthermore, for all $I \in \binom{n}{2}$, we have $f_I = (f_{\mathrm{aff}})_I + (f_{\mathrm{non}})_I$. Since f is not affine, it holds that $P_{\mathrm{non}} \neq 0$.

Assume first that P_{non} has a monomial $M = a_{\mathbf{r}}\mathbf{x}^{\mathbf{r}}$ in which there occur at most $n-2$ variables, i.e., $a_{\mathbf{r}} \neq 0$ and there exist $i,j \in [n]$ such that $i \neq j$ and $r_i = r_j = 0$. Let $I = \{i,j\}$. The canonical polynomial of f_I contains the monomial M (with some reindexing of variables, if necessary); hence f_I is not affine.

Assume then that all monomials in P_{non} have at least $n-1$ variables. If there is a variable x_i with $i \in [n]$ that does not occur in any of the monomials of P_{non}, then let $I = \{i,j\}$ for any $j \in [n]\setminus\{i\}$. The canonical polynomial of f_I contains all monomials of P_{non} (with some reindexing of variables, if necessary); hence f_I is not affine.

We are left with the case that all monomials in P_{non} have at least $n-1$ variables and all variables x_i, $i \in [n]$, occur in P_{non}. Identification of a pair of variables in P_{non} results in a polynomial in which all monomials have at least $n-2$ variables; some monomials may cancel each other, so the resulting polynomial may be 0. Since f_{non} depends on all of its n arguments and $n > \max(q,3)$, it follows from Lemma 4.1 that there exists $I \in \binom{n}{2}$ such that $(f_{\mathrm{non}})_I$ depends on at least $n-2$ arguments; hence the canonical polynomial of $(f_{\mathrm{non}})_I$ cannot be 0, so it contains a monomial with at least $n-2$ variables. Consequently, the canonical polynomial of f_I has a monomial with at least $n-2$ variables; hence f_I is not affine. □

Theorem 4.7. *Let $(G;+,\cdot)$ be a finite field of order $q = p^k$. The affine functions of arity at least $\max(q,3)+1$ over $(G;+,\cdot)$ are reconstructible.*

Proof. Let $\mathcal{C}$ be the class of affine functions of arity at least $\max(q,3)+1$ over $(G;+,\cdot)$. Since the identification minors of affine functions are affine, Lemma 4.6 implies that $\mathcal{C}$ is recognizable. By Theorem 4.5, $\mathcal{C}$ is weakly reconstructible. Consequently, $\mathcal{C}$ is reconstructible. □

Remark 4.8. The lower bound $\max(q,3)+1$ in Theorem 4.7 cannot be improved. As explained in [7], no function $f\colon A^n \to B$ with $n \leq |A|$ is reconstructible. It is also necessary to assume that the arity is greater than 3. Since $(G;+)$ is a group, additive inverses exist for all elements, and for all $a,b \in G$, the multisets $\langle a,b,-(a+b)\rangle$ and $\langle -a,-b,a+b\rangle$ have the same deck (see Example 3.3); thus the affine functions

induced by the polynomials $ax_1 + bx_2 - (a+b)x_3$ and $-ax_1 - bx_2 + (a+b)x_3$ have the same deck.

Furthermore, if $(G; +, \cdot)$ is the two-element field, then $(G; +)$ is a Boolean group, and the multisets $\langle 1, 1, 1\rangle$ and $\langle 1, 0, 0\rangle$ have the same deck (see Example 3.2). Thus the ternary functions induced by the polynomials $x_1 + x_2 + x_3$ and x_1 have the same deck, because all identification minors of these functions are projections, and any two projections are equivalent. The class of affine functions of arity 3 on the 2-element field is not even recognizable. Namely, all identification minors of the function induced by the polynomial $x_1x_2 + x_1x_3 + x_2x_3$ are projections, too.

Remark 4.9. As explained in [7], if A is infinite, then no function $f\colon A^n \to B$ is reconstructible. Even the class of polynomial functions over an infinite field F fails to be weakly reconstructible. For $n \geq 2$, define the polynomial function $\Delta_n\colon F^n \to F$,

$$\Delta_n(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

We have that $(\Delta_n)_I(x_1, \ldots, x_{n-1}) = 0$ for every $I \in \binom{n}{2}$. Consequently, for any function $f\colon F^n \to F$ (polynomial or not), it holds that $f_I = (f + \Delta_n)_I$ for every $I \in \binom{n}{2}$ and $\operatorname{deck} f = \operatorname{deck}(f + \Delta_n)$.

Acknowledgments

The author would like to thank Miguel Couceiro for inspiring discussions on minors of functions and reconstruction problems.

References

[1] M. Bouaziz, M. Couceiro and M. Pouzet, Join-irreducible Boolean functions, *Order* **27** (2010) 261–282.
[2] M. Couceiro and S. Foldes, On closed sets of relational constraints and classes of functions closed under variable substitutions, *Algebra Universalis* **54** (2005) 149–165.
[3] M. Couceiro and E. Lehtonen, Generalizations of Świerczkowski's lemma and the arity gap of finite functions, *Discrete Math.* **309** (2009) 5905–5912.
[4] O. Ekin, S. Foldes, P. L. Hammer and L. Hellerstein, Equational characterizations of Boolean functions classes, *Discrete Math.* **211** (2000) 27–51.
[5] P. J. Kelly, *On Isometric Transformations,* Ph.D. thesis (University of Wisconsin, 1942).
[6] S. Lang, *Algebra* (Springer, New York, 2002).
[7] E. Lehtonen, On the reconstructibility of totally symmetric functions and of other functions with a unique identification minor, arXiv:1208.3110.
[8] E. Lehtonen and Á. Szendrei, Partial orders induced by quasilinear clones, *Contributions to General Algebra* **20**, Proceedings of the Salzburg Conference 2011 (AAA81) (Verlag Johannes Heyn, Klagenfurt, 2012), pp. 51–84.
[9] S. Mac Lane and G. Birkhoff, *Algebra,* 3rd ed. (Chelsea Publishing Co., New York, 1988).
[10] N. Pippenger, Galois theory for minors of finite functions, *Discrete Math.* **254** (2002) 405–419.
[11] M. D. Prešić, On free commutative groupoids, *Publ. Inst. Math. (Beograd) (N.S.)* **27(41)** (1980) 209–223.
[12] S. M. Ulam, *A Collection of Mathematical Problems,* (Interscience Publishers, New York, 1960).
[13] C. Wang, Boolean minors, *Discrete Math.* **141** (1995) 237–258.
[14] R. Willard, Essential arities of term operations in finite algebras, *Discrete Math.* **149** (1996) 239–259.
[15] I. E. Zverovich, Characterizations of closed classes of Boolean functions in terms of forbidden subfunctions and Post classes, *Discrete Appl. Math.* **149** (2005) 200–218.

(E. Lehtonen) Computer Science and Communications Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L–1359 Luxembourg, Luxembourg
E-mail address: erkko.lehtonen@uni.lu