Reconstructing functions from identification minors

Erkko Lehtonen

University of Luxembourg
erkko.lehtonen@uni.lu

joint work with
Miguel Couceiro (Université Paris-Dauphine)
Karsten Schölzel (University of Luxembourg)

The 4th Novi Sad Algebraic Conference
Novi Sad, June 5–9, 2013

Identification minors

Assume that $n \geq 2$, and let $f\colon A^n \to B$.

For each $I \in \binom{n}{2}$, define the function $f_I\colon A^{n-1} \to B$ as

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

for all $a_1, \ldots, a_{n-1} \in A$.

The function f_I is referred to as an identification minor of f.

Functions $f\colon A^n \to B$ and $g\colon A^n \to B$ are equivalent if there exists a permutation $\sigma\colon [n] \to [n]$ such that

$$f(a_1, \ldots, a_n) = g(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$$

for all $a_1, \ldots, a_n \in A^n$.

Identification minors

Assume that $n \geq 2$, and let $f\colon A^n \to B$.

For each $I \in \binom{n}{2}$, define the function $f_I\colon A^{n-1} \to B$ as

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

for all $a_1, \ldots, a_{n-1} \in A$.

The function f_I is referred to as an identification minor of f.

Functions $f\colon A^n \to B$ and $g\colon A^n \to B$ are equivalent if there exists a permutation $\sigma\colon [n] \to [n]$ such that

$$f(a_1, \ldots, a_n) = g(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$$

for all $a_1, \ldots, a_n \in A^n$.

Identification minors – examples

Example

Let $f\colon \mathbb{R}^3 \to \mathbb{R}$, $f(x_1, x_2, x_3) = x_1 x_2 - x_1 x_3$.

The identification minors of f are the following:

$$\begin{aligned} f_{\{1,2\}}(x_1, x_2) &= x_1^2 - x_1 x_2, \\ f_{\{1,3\}}(x_1, x_2) &= x_1 x_2 - x_1^2, \\ f_{\{2,3\}}(x_1, x_2) &= 0. \end{aligned}$$

Identification minors – examples

Example

Let $n \geq 2$ and let $f\colon \{0,1\}^n \to \{0,1\}$ be given by the rule

$$f(x_1, \dots, x_n) = x_1 + x_2 + \cdots + x_n$$

(addition modulo 2).

For every $I \in \binom{n}{2}$, the identification minor f_I is equivalent to the function $g\colon \{0,1\}^{n-1} \to \{0,1\}$,

$$g(x_1, \dots, x_{n-1}) = x_1 + \cdots + x_{n-2}.$$

Reconstruction problem for functions

Assume that $n \geq 2$ and $f\colon A^n \to B$.

1. The deck of f, denoted $\operatorname{deck} f$, is the multiset $\{f_I/{\equiv} : I \in \binom{n}{2}\}$. Any element of the deck of f is called a card of f.
2. A function $g\colon A^n \to B$ is a reconstruction of f, if $\operatorname{deck} f = \operatorname{deck} g$.
3. A function is reconstructible if it is equivalent to all of its reconstructions.
4. A class $\mathcal{C} \subseteq \mathcal{F}_{AB}$ of functions is reconstructible, if all members of $\mathcal{C}$ are reconstructible.
5. 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.
6. A class $\mathcal{C} \subseteq \mathcal{F}_{AB}$ is recognizable, if all reconstructions of members of $\mathcal{C}$ are members of $\mathcal{C}$.

Reconstruction problem for functions

Question

Let A and B be sets with at least two elements, and let n be an integer greater than or equal to 2. Is every function $f\colon A^n \to B$ reconstructible?

Reconstruction problem for functions

Let $f\colon A^n \to B$. If $n \leq |A|$, then the set

$$A^n_{\neq} := \{(a_1, \dots, a_n) \in A^n : a_i \neq a_j \text{ whenever } i \neq j\}$$

is nonempty.

The points in $A^n_{\neq}$ play no role in the identification minors of f.

Therefore, if $g\colon A^n \to B$ is another function such that $f(\mathbf{a}) = g(\mathbf{a})$ for all $\mathbf{a} \in A^n \setminus A^n_{\neq}$, then $\operatorname{deck} f = \operatorname{deck} g$. Thus, for every $f\colon A^n \to B$, it is easy to devise a function $g\colon A^n \to B$ such that $f \neq g$ and $\operatorname{deck} f = \operatorname{deck} g$.

Thus, the answer to the Question is negative unless $n > |A|$.

This also shows that if A is infinite, then no function $f\colon A^n \to B$ is reconstructible.

Reconstruction problem for functions

Let $f\colon A^n \to B$. If $n \leq |A|$, then the set

$$A^n_{\neq} := \{(a_1, \dots, a_n) \in A^n : a_i \neq a_j \text{ whenever } i \neq j\}$$

is nonempty.

The points in $A^n_{\neq}$ play no role in the identification minors of f.

Therefore, if $g\colon A^n \to B$ is another function such that $f(\mathbf{a}) = g(\mathbf{a})$ for all $\mathbf{a} \in A^n \setminus A^n_{\neq}$, then $\operatorname{deck} f = \operatorname{deck} g$. Thus, for every $f\colon A^n \to B$, it is easy to devise a function $g\colon A^n \to B$ such that $f \neq g$ and $\operatorname{deck} f = \operatorname{deck} g$.

Thus, the answer to the Question is negative unless $n > |A|$.

This also shows that if A is infinite, then no function $f\colon A^n \to B$ is reconstructible.

Reconstruction problem for functions

Let $f\colon A^n \to B$. If $n \leq |A|$, then the set

$$A^n_{\neq} := \{(a_1, \dots, a_n) \in A^n : a_i \neq a_j \text{ whenever } i \neq j\}$$

is nonempty.

The points in $A^n_{\neq}$ play no role in the identification minors of f.

Therefore, if $g\colon A^n \to B$ is another function such that $f(\mathbf{a}) = g(\mathbf{a})$ for all $\mathbf{a} \in A^n \setminus A^n_{\neq}$, then $\operatorname{deck} f = \operatorname{deck} g$. Thus, for every $f\colon A^n \to B$, it is easy to devise a function $g\colon A^n \to B$ such that $f \not\equiv g$ and $\operatorname{deck} f = \operatorname{deck} g$.

Thus, the answer to the Question is negative unless $n > |A|$.

This also shows that if A is infinite, then no function $f\colon A^n \to B$ is reconstructible.

Reconstruction problem for functions

Let $f\colon A^n \to B$. If $n \leq |A|$, then the set

$$A^n_{\neq} := \{(a_1, \dots, a_n) \in A^n : a_i \neq a_j \text{ whenever } i \neq j\}$$

is nonempty.

The points in $A^n_{\neq}$ play no role in the identification minors of f.

Therefore, if $g\colon A^n \to B$ is another function such that $f(\mathbf{a}) = g(\mathbf{a})$ for all $\mathbf{a} \in A^n \setminus A^n_{\neq}$, then $\operatorname{deck} f = \operatorname{deck} g$. Thus, for every $f\colon A^n \to B$, it is easy to devise a function $g\colon A^n \to B$ such that $f \neq g$ and $\operatorname{deck} f = \operatorname{deck} g$.

Thus, the answer to the Question is negative unless $n > |A|$.

This also shows that if A is infinite, then no function $f\colon A^n \to B$ is reconstructible.

Reconstruction problem for functions

Let $f\colon A^n \to B$. If $n \leq |A|$, then the set

$$A^n_{\neq} := \{(a_1, \dots, a_n) \in A^n : a_i \neq a_j \text{ whenever } i \neq j\}$$

is nonempty.

The points in $A^n_{\neq}$ play no role in the identification minors of f.

Therefore, if $g\colon A^n \to B$ is another function such that $f(\mathbf{a}) = g(\mathbf{a})$ for all $\mathbf{a} \in A^n \setminus A^n_{\neq}$, then $\operatorname{deck} f = \operatorname{deck} g$. Thus, for every $f\colon A^n \to B$, it is easy to devise a function $g\colon A^n \to B$ such that $f \not\equiv g$ and $\operatorname{deck} f = \operatorname{deck} g$.

Thus, the answer to the Question is negative unless $n > |A|$.

This also shows that if A is infinite, then no function $f\colon A^n \to B$ is reconstructible.

Functions with a unique identification minor

A function $f \colon A^n \to B$ has a unique identification minor, if $f_I \equiv f_J$ for all $I, J \in \binom{n}{2}$.

Example

Functions with a unique identification minor:

- 2-set-transitive functions,
- functions weakly determined by the order of first occurrence.

Problem

Determine all functions with a unique identification minor.

Functions with a unique identification minor

A function $f\colon A^n \to B$ has a unique identification minor, if $f_I \equiv f_J$ for all $I, J \in \binom{n}{2}$.

Example

Functions with a unique identification minor:

- 2-set-transitive functions,
- functions weakly determined by the order of first occurrence.

Problem

Determine all functions with a unique identification minor.

Functions with a unique identification minor

A function $f\colon A^n \to B$ has a unique identification minor, if $f_I \equiv f_J$ for all $I, J \in \binom{n}{2}$.

Example

Functions with a unique identification minor:

- 2-set-transitive functions,
- functions weakly determined by the order of first occurrence.

Problem

Determine all functions with a unique identification minor.

Invariance groups

A function $f\colon A^n \to B$ is invariant under a permutation $\sigma \in \Sigma_n$, if for all $a_1, \dots, a_n \in A$, it holds that

$$f(a_1, \dots, a_n) = f(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

The set of all permutations under which f is invariant is denoted by $\operatorname{Inv} f$.

$(\operatorname{Inv} f; \circ)$ is a group, called the invariance group of f.

A function f is totally symmetric, if $\operatorname{Inv} f = \Sigma_n$.

A permutation group G is 2-set-transitive if for all $I, J \in \binom{n}{2}$, there exists a permutation $\sigma \in G$ such that $\sigma[I] = J$.

A function f is 2-set-transitive if $\operatorname{Inv} f$ is 2-set-transitive.

Invariance groups

A function $f\colon A^n \to B$ is invariant under a permutation $\sigma \in \Sigma_n$, if for all $a_1, \dots, a_n \in A$, it holds that

$$f(a_1, \dots, a_n) = f(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

The set of all permutations under which f is invariant is denoted by $\operatorname{Inv} f$.
$(\operatorname{Inv} f; \circ)$ is a group, called the invariance group of f.

A function f is totally symmetric, if $\operatorname{Inv} f = \Sigma_n$.

A permutation group G is 2-set-transitive if for all $I, J \in \binom{n}{2}$, there exists a permutation $\sigma \in G$ such that $\sigma[I] = J$.

A function f is 2-set-transitive if $\operatorname{Inv} f$ is 2-set-transitive.

Invariance groups

A function $f\colon A^n \to B$ is invariant under a permutation $\sigma \in \Sigma_n$, if for all $a_1, \dots, a_n \in A$, it holds that

$$f(a_1, \dots, a_n) = f(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

The set of all permutations under which f is invariant is denoted by $\operatorname{Inv} f$.
$(\operatorname{Inv} f; \circ)$ is a group, called the invariance group of f.

A function f is totally symmetric, if $\operatorname{Inv} f = \Sigma_n$.

A permutation group G is 2-set-transitive if for all $I, J \in \binom{n}{2}$, there exists a permutation $\sigma \in G$ such that $\sigma[I] = J$.

A function f is 2-set-transitive if $\operatorname{Inv} f$ is 2-set-transitive.

Invariance groups

A function $f\colon A^n \to B$ is invariant under a permutation $\sigma \in \Sigma_n$, if for all $a_1, \dots, a_n \in A$, it holds that

$$f(a_1, \dots, a_n) = f(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

The set of all permutations under which f is invariant is denoted by $\operatorname{Inv} f$.
$(\operatorname{Inv} f; \circ)$ is a group, called the invariance group of f.

A function f is totally symmetric, if $\operatorname{Inv} f = \Sigma_n$.

A permutation group G is 2-set-transitive if for all $I, J \in \binom{n}{2}$, there exists a permutation $\sigma \in G$ such that $\sigma[I] = J$.

A function f is 2-set-transitive if $\operatorname{Inv} f$ is 2-set-transitive.

Functions determined by the order of first occurrence

We define the map $\mathrm{ofo} \colon \bigcup_{n \geq 1} A^n \to \bigcup_{n \geq 1} A^n_{\neq}$ as follows:
given a tuple $\mathbf{a} \in A^n$, $\mathrm{ofo}(\mathbf{a})$ is the tuple obtained from $\mathbf{a}$ by removing all repeated occurrences of elements in $\mathbf{a}$, retaining only the first occurrence of each element.

Example

$\mathrm{ofo}(1, 3, 5, 7, 9) = (1, 3, 5, 7, 9)$
$\mathrm{ofo}(2, 0, 1, 3, 0, 6, 0, 7) = (2, 0, 1, 3, 6, 7)$
$\mathrm{ofo}(3, 5, 2, 4, 6, 6, 6, 4, 4, 6, 8, 4, 8) = (3, 5, 2, 4, 6, 8)$

Functions determined by the order of first occurrence

We say that $f\colon A^n \to B$ is determined by the order of first occurrence if there exists a map $f^*\colon \bigcup_{n \geq 1} A^n_{\neq} \to B$ such that $f = f^* \circ \mathrm{ofo}|_{A^n}$.

We say that $f\colon A^n \to B$ is weakly determined by the order of first occurrence if there exists a function $g\colon A^n \to B$ that is determined by the order of first occurrence and $f \equiv g$.

Functions determined by the order of first occurrence

We say that $f\colon A^n \to B$ is determined by the order of first occurrence if there exists a map $f^*\colon \bigcup_{n \geq 1} A^n_{\neq} \to B$ such that $f = f^* \circ \mathrm{ofo}|_{A^n}$.

We say that $f\colon A^n \to B$ is weakly determined by the order of first occurrence if there exists a function $g\colon A^n \to B$ that is determined by the order of first occurrence and $f \equiv g$.

Some reconstructible families of functions

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f \colon A^n \to B$ is totally symmetric, then f is reconstructible.

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f \colon A^n \to B$ is determined by $(\mathrm{pr}, \mathrm{supp})$, then f is reconstructible.

Theorem

Assume that n and k are positive integers such that

- $k \equiv 1, 2 \pmod{4}$ *and* $n \geq k + 2$, *or*
- $k \equiv 0, 3 \pmod{4}$ *and* $n \geq k + 3$.

Let $f, g \colon A^n \to B$ be functions that are weakly determined by the order of first occurrence. If $\operatorname{deck} f = \operatorname{deck} g$, then $f = g$.

Some reconstructible families of functions

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f\colon A^n \to B$ is totally symmetric, then f is reconstructible.

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f\colon A^n \to B$ is determined by $(\mathrm{pr}, \mathrm{supp})$, then f is reconstructible.

Theorem

Assume that n and k are positive integers such that

- $k \equiv 1, 2 \pmod{4}$ *and* $n \geq k + 2$, *or*
- $k \equiv 0, 3 \pmod{4}$ *and* $n \geq k + 3$.

Let $f, g\colon A^n \to B$ be functions that are weakly determined by the order of first occurrence. If $\operatorname{deck} f = \operatorname{deck} g$, then $f \equiv g$.

Some reconstructible families of functions

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f \colon A^n \to B$ is totally symmetric, then f is reconstructible.

Theorem

Assume that $n \geq k + 2$ and $|A| = k$. If $f \colon A^n \to B$ is determined by $(\mathrm{pr}, \mathrm{supp})$, then f is reconstructible.

Theorem

Assume that n and k are positive integers such that

- $k \equiv 1, 2 \pmod 4$ *and* $n \geq k + 2$, *or*
- $k \equiv 0, 3 \pmod 4$ *and* $n \geq k + 3$.

Let $f, g \colon A^n \to B$ be functions that are weakly determined by the order of first occurrence. If $\operatorname{deck} f = \operatorname{deck} g$, then $f \equiv g$.

Linear and affine functions

Let $(A; +, \cdot)$ be a nonassociative right semiring, i.e., an algebra such that

- $(A; +)$ is a commutative monoid with neutral element 0,
- $(A; \cdot)$ is a groupoid with right identity 1,
- $(a + b) \cdot c = a \cdot c + b \cdot c$,
- $a \cdot 0 = 0$.

$(A; +, \cdot)$ is cancellative if $a + b = a + c$ implies $b = c$.

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

$$f(x_1, \ldots, x_n) = a_1 x_2 + \cdots + a_n x_n + c$$

for some $a_1, \ldots a_n, c \in A$. If $c = 0$, then f is linear.

Linear and affine functions

Let $(A; +, \cdot)$ be a nonassociative right semiring, i.e., an algebra such that

- $(A; +)$ is a commutative monoid with neutral element 0,
- $(A; \cdot)$ is a groupoid with right identity 1,
- $(a + b) \cdot c = a \cdot c + b \cdot c$,
- $a \cdot 0 = 0$.

$(A; +, \cdot)$ is cancellative if $a + b = a + c$ implies $b = c$.

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

$$f(x_1, \dots, x_n) = a_1 x_2 + \cdots + a_n x_n + c$$

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

Linear and affine functions

An affine function is uniquely determined (up to equivalence) by the multiset of its coefficients $a_1, \ldots, a_n$ and the constant term c.

The reconstruction problem for affine functions is essentially the same thing as a reconstruction problem for multisets as formulated below.

Let $(A; +)$ be a commutative groupoid. Let $M = \langle m_1, \ldots, m_n \rangle$ be a multiset of cardinality $n \geq 2$ over A. The cards of M are the multisets of cardinality $n - 1$ of the form

$$M \setminus \langle m_i, m_j \rangle \uplus \langle m_i + m_j \rangle$$

for all $\{i, j\} \in \binom{n}{2}$.

Linear and affine functions

Theorem

Let $(A; +)$ be a commutative groupoid, and let M and M' be multisets of cardinality n over A. Then $\operatorname{deck} M = \operatorname{deck} M'$ if and only if $M = M'$ or

- *$n = 2$ and $M = \langle r, s \rangle$, $M' = \langle t, u \rangle$ for some $r, s, t, u \in A$ satisfying $r + s = t + u$;*
- *$n = 3$ and $M = \langle r, s, t \rangle$, $M' = \langle r, r + s, r + t \rangle$ for some $r, s, t \in A$ satisfying $r + (r + s) = s$, $r + (r + t) = t$, $(r + s) + (r + t) = s + t$;*
- *$n = 3$ and $M = \langle r, s, t \rangle$, $M' = \langle r + s, r + t, s + t \rangle$ for some $r, s, t \in A$ satisfying $(r + s) + (r + t) = r$, $(r + s) + (s + t) = s$, $(r + t) + (s + t) = t$;*
- *$n = 4$ and $M = \langle r, s, t, u \rangle$, $M' = \langle r, s, t, v \rangle$ for some $r, s, t, u, v \in A$ satisfying $x + u = v$ and $x + v = u$ for all $x \in \{r, s, t\}$ and $r + s = s$, $s + t = t$, $t + r = r$.*

Linear and affine functions

Theorem

Let $f, g \colon A^n \to A$ be affine functions over a nonassociative right semiring $(A; +, \cdot)$ 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 $f \equiv g$.

Theorem

Let $(A; +, \cdot)$ be a finite field of order q. The class of affine functions over $(A; +, \cdot)$ of arity at least $\max(q, 3) + 1$ is reconstructible.

Monotone functions

An important special case of monotone functions are the term operations of a distributive lattice. Each such operation has a unique representation of the form

$$\bigvee_{S \in \mathcal{S}} \Big(\bigwedge_{i \in S} x_i \Big)$$

where $\mathcal{S} \subseteq \mathcal{P}([n])$ satisfies the condition that no member of $\mathcal{S}$ is a subset of another member of $\mathcal{S}$.

Monotone Boolean functions are precisely the term operations of the two-element lattice.

It is useful to formulate the reconstruction problem of monotone functions in terms of Sperner systems, i.e., antichains in the power set lattice $(\mathcal{P}(A); \subseteq)$.

Monotone functions

Example

Let $f = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$.
This corresponds to the Sperner system

$$\mathcal{A} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

over the set $\{1, 2, 3\}$.

The cards of $\mathcal{A}$ are

$$\mathcal{A}_{12} = \{\{1\}\}, \quad \mathcal{A}_{13} = \{\{1\}\}, \quad \mathcal{A}_{23} = \{\{2\}\},$$

all of which are isomorphic to the Sperner system $\{\{1\}\}$ over $\{1, 2\}$.

These correspond to projections, which are identification minors of f.

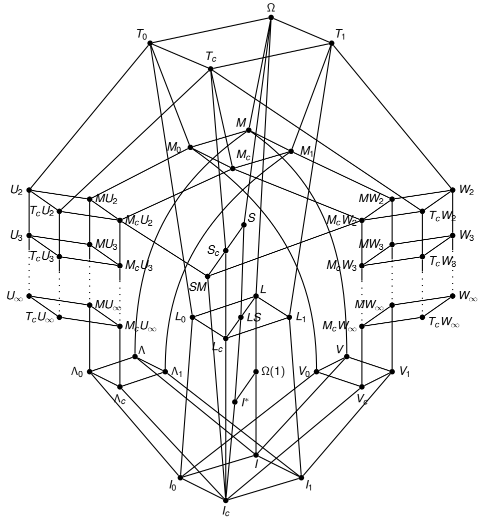
Monotone functions

We have constructed infinite families of nonreconstructible Sperner systems.

These translate into families of nonreconstructible distributive lattice polynomial operations, in particular, monotone Boolean functions.

This was done in different ways so that for one of our families the associated Boolean functions are members of the clone SM, and for another family they are members of $M_c U_\infty$.

Reconstructibility of the clones on $\{0, 1\}$



Theorem

Let $\mathcal{C}$ be a clone on $\{0, 1\}$.

If $\mathcal{C}$ contains SM, M_cU_∞ or M_cW_∞, then $\mathcal{C}^{(\geq n)}$ is not weakly reconstructible for every $n \geq 1$.

Otherwise (i.e., $\mathcal{C}$ is contained in L, Λ or V) $\mathcal{C}^{(\geq 4)}$ is reconstructible.

Thank you for your attention!