AUTOMATIZING PROOFS OF PROPERTIES OF OPERATORS

Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger

Johannes Kepler University, Linz, Austria

AADIOS @ ACA

Online, 27 July 2021

JOHANNES KEPLER UNIVERSITY LINZ

FWF Der Wissenschaftsfonds.

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?

statement about operators

$\downarrow$

assumptions

$\Rightarrow$

claim

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?

statement about operators

$\downarrow$ formal computation

assumptions $\Rightarrow$ claim

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?

statement about operators $\xrightarrow{\text{translate}}$ noncommutative polynomials

formal computation $\downarrow$

assumptions

$\Rightarrow$

claim

Motivation

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?

statement about operators $\xrightarrow{\text{translate}}$ noncommutative polynomials

statement about operators $\xrightarrow{\text{formal computation}}$ assumptions $\Rightarrow$ claim

noncommutative polynomials $\xrightarrow{\text{solve}}$ statement about polynomials

Motivation

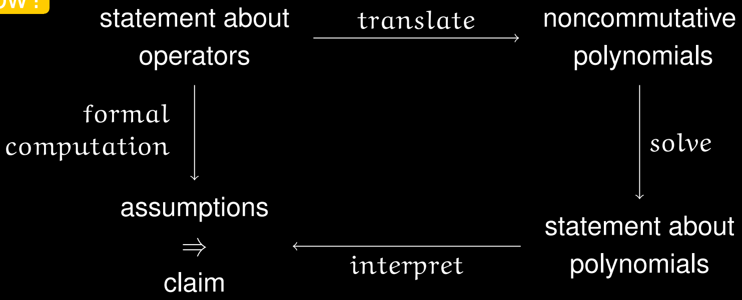
Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?



Motivation

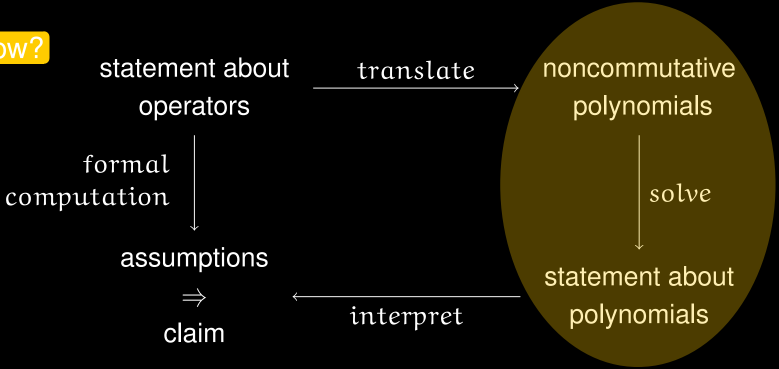
Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Goal

Prove such statements automatically!

How?



Framework for verifying operator statements

(Raab, Regensburger, Hossein Poor, 2021)

Starting point: Statement about matrices or operators to prove

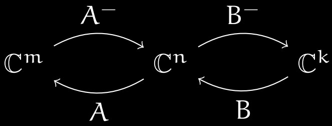
1. Translation:
    1. Phrase all properties in terms of identities
    2. Convert identities into noncommutative polynomials
2. Solving: Verify ideal membership of claim
3. Interpretation: Consider different settings

More formally...

Setting is encoded in labelled quiver Q.

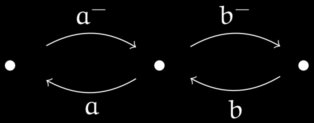
More formally. . .

Setting is encoded in labelled quiver Q.



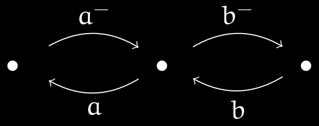
More formally...

Setting is encoded in labelled quiver Q.



More formally...

Setting is encoded in labelled quiver Q.

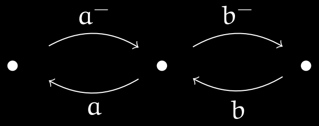


Quiver representations in an R-linear category

Vertices and edges of Q are assigned objects and morphisms.

More formally...

Setting is encoded in labelled quiver Q.



Quiver representations in an $\mathbb{R}$-linear category

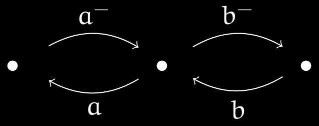
Vertices and edges of Q are assigned objects and morphisms.

$f \in R\langle X \rangle$ compatible with $Q \iff$ monomials of f are paths in Q with same start and end.

$\Rightarrow$ Compatible polynomials have realizations as morphisms.

More formally...

Setting is encoded in labelled quiver Q.



Quiver representations in an R-linear category

Vertices and edges of Q are assigned objects and morphisms.

$f \in R\langle X\rangle$ compatible with $Q \iff$ monomials of f are paths in Q with same start and end.

$\Rightarrow$ Compatible polynomials have realizations as morphisms.

Theorem (Raab, Regensburger, Hossein Poor, 2021)

Let $F \subseteq R\langle X\rangle$ and $f \in (F)$. Then, for every labelled quiver Q and every representation of Q in an R-linear category s.t.

1. f and all elements of F are compatible with Q, and
2. realizations of all elements of F are zero,

we have that the realization of f is zero.

Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Assumptions:

$$AA^-A = A, \qquad BB^-B = B, \qquad (A^-ABB^-)^2 = A^-ABB^-$$

Claim:

$$ABB^-A^-AB = AB$$

Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Assumptions:

$$aa^-a - a, \qquad bb^-b - b, \qquad (a^-abb^-)^2 - a^-abb^-$$

Claim:

$$abb^-a^-ab - ab$$

Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Assumptions:

$$aa^-a - a, \qquad bb^-b - b, \qquad (a^-abb^-)^2 - a^-abb^-$$

Claim:

$$abb^-a^-ab - ab$$

Then, "assumptions $\Rightarrow$ claim" since

$$f = f_1(bb^-b - bb^-a^-abb^-b) + (a - abb^-a^-a)f_2 + af_3b.$$

Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Assumptions:

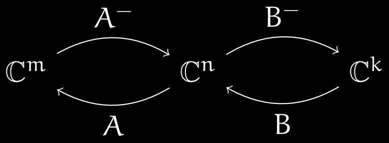
$$aa^-a - a, \qquad bb^-b - b, \qquad (a^-abb^-)^2 - a^-abb^-$$

Claim:

$$abb^-a^-ab - ab$$

Then, “assumptions $\Rightarrow$ claim” since

$$f = f_1(bb^-b - bb^-a^-abb^-b) + (a - abb^-a^-a)f_2 + af_3b.$$



Example revisited

Theorem (Werner, 1994)

Let $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times k}$ with inner inverses A^- and B^-. If A^-ABB^- is idempotent, then B^-A^- is an inner inverse of AB.

Assumptions:

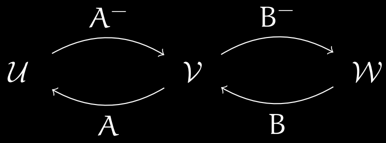
$$aa^-a - a, \qquad bb^-b - b, \qquad (a^-abb^-)^2 - a^-abb^-$$

Claim:

$$abb^-a^-ab - ab$$

Then, “assumptions $\Rightarrow$ claim” since

$$f = f_1(bb^-b - bb^-a^-abb^-b) + (a - abb^-a^-a)f_2 + af_3b.$$



Applications

Framework implemented in the MATHEMATICA and SAGEMATH package `OperatorGB`. Available at

`https://clemenshofstadler.com/software/`

Successfully used to automatically (im)prove statements in the field of

- generalised inverses (more specifically: reverse order laws)
- homological algebra (more specifically: diagram chases)

Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^{\dagger}ABCC^{\dagger}$ and $Q = CC^{\dagger}B^{\dagger}A^{\dagger}A$.
Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

$$M^{\dagger} = C^{\dagger}B^{\dagger}A^{\dagger}.$$

Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^{\dagger}ABCC^{\dagger}$ and $Q = CC^{\dagger}B^{\dagger}A^{\dagger}A$.

Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

$$M^{\dagger} = C^{\dagger}B^{\dagger}A^{\dagger}.$$

Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^\dagger ABCC^\dagger$ and $Q = CC^\dagger B^\dagger A^\dagger A$.
Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

$$M^\dagger = C^\dagger B^\dagger A^\dagger.$$

Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Proof of sufficiency in $\mathbb{Q}\langle X\rangle$ with $|X| = 22$:

Assumptions: $f_1, \ldots, f_{34}$
with $\max_i \deg(f_i) = 20$

Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^\dagger ABCC^\dagger$ and $Q = CC^\dagger B^\dagger A^\dagger A$. Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

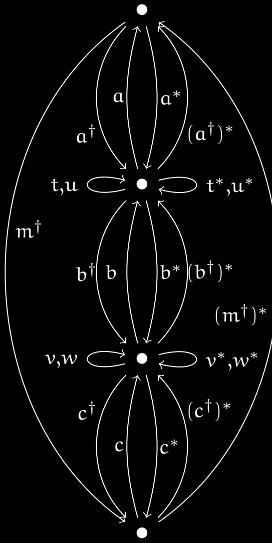
$$M^\dagger = C^\dagger B^\dagger A^\dagger.$$

Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Proof of sufficiency in $\mathbb{Q}\langle X \rangle$ with $|X| = 22$:

Assumptions: $f_1, \ldots, f_{34}$

with $\max_i \deg(f_i) = 20$



Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^\dagger ABCC^\dagger$ and $Q = CC^\dagger B^\dagger A^\dagger A$. Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

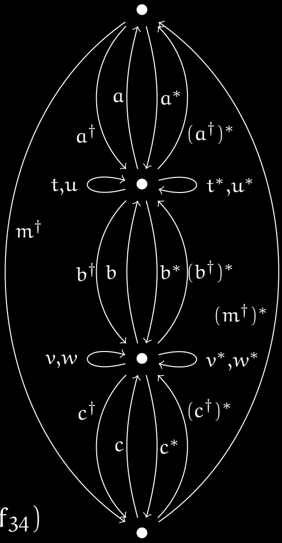
$$M^\dagger = C^\dagger B^\dagger A^\dagger.$$

Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Proof of sufficiency in $\mathbb{Q}\langle X\rangle$ with $|X| = 22$:

Assumptions: $f_1, \ldots, f_{34}$
with $\max_i \deg(f_i) = 20$

Claim: $h := m^\dagger - c^\dagger b^\dagger a^\dagger$, Verify: $h \in (f_1, \ldots, f_{34})$



Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^\dagger ABCC^\dagger$ and $Q = CC^\dagger B^\dagger A^\dagger A$.
Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$ iff

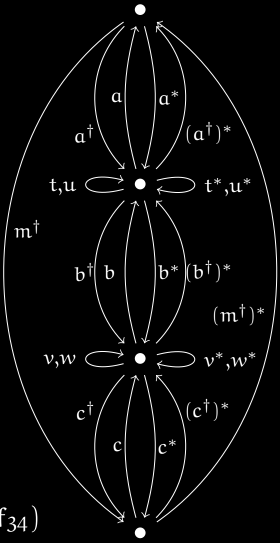
$$M^\dagger = C^\dagger B^\dagger A^\dagger.$$

Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Proof of sufficiency in $\mathbb{Q}\langle X \rangle$ with $|X| = 22$:

Assumptions: $f_1, \ldots, f_{34}$
with $\max_i \deg(f_i) = 20$

Claim: $h := m^\dagger - c^\dagger b^\dagger a^\dagger$, Verify: $h \in (f_1, \ldots, f_{34})$



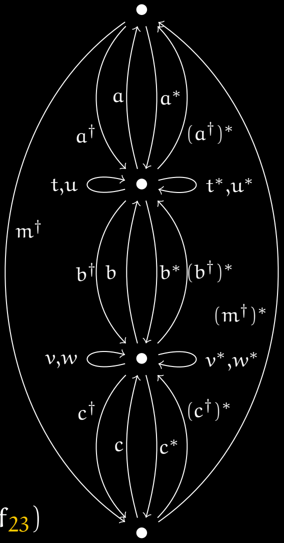
Interpretation: matrices, Hilbert spaces, involutive categories,...

Example: product of three Moore-Penrose inverses

Theorem (Hartwig, 1986)

A, B, C matrices s.t. $M = ABC$ exists. Let $P = A^\dagger ABCC^\dagger$ and $Q = CC^\dagger B^\dagger A^\dagger A$.
Then, $PQ = (PQ)^2, \mathcal{R}(A^*AP) \supseteq \mathcal{R}(Q^*)$, $\mathcal{R}(CC^*P^*) \subseteq \mathcal{R}(Q)$ iff

$$M^\dagger = C^\dagger B^\dagger A^\dagger.$$



Translation: $\mathcal{R}(X) \subseteq \mathcal{R}(Y) \Leftrightarrow \exists Z : X = YZ$

Proof of sufficiency in $\mathbb{Q}\langle X\rangle$ with $|X| = 20$:

Assumptions: $f_1, \ldots, f_{23}$
with $\max_i \deg(f_i) = 20$

Claim: $h := m^\dagger - c^\dagger b^\dagger a^\dagger$, Verify: $h \in (f_1, \ldots, f_{23})$

Interpretation: matrices, Hilbert spaces, involutive categories,...

Example: Five lemma

Theorem (Five lemma)

Consider the following commutative diagram with exact rows in an abelian category.

If α is an epimorphism,
β, δ are isomorphisms
and ε is a monomorphism,
then γ is an isomorphism.

$$\begin{array}{ccccccccc}
A & \xrightarrow{a} & B & \xrightarrow{b} & C & \xrightarrow{c} & D & \xrightarrow{d} & E \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\
A' & \xrightarrow[a']{} & B' & \xrightarrow[b']{} & C' & \xrightarrow[c']{} & D' & \xrightarrow[d']{} & E'
\end{array}$$

Example: Five lemma

Theorem (Five lemma)

Consider the following commutative diagram with exact rows in an abelian category.

If α is an epimorphism,
β, δ are isomorphisms
and ε is a monomorphism,
then γ is an isomorphism.

$$\begin{array}{ccccccccc} A & \xrightarrow{a} & B & \xrightarrow{b} & C & \xrightarrow{c} & D & \xrightarrow{d} & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ A' & \xrightarrow[a']{} & B' & \xrightarrow[b']{} & C' & \xrightarrow[c']{} & D' & \xrightarrow[d']{} & E' \end{array}$$

- f monomorphism iff $\forall g : fg = 0 \Rightarrow g = 0$
- f epimorphism iff $\forall g : gf = 0 \Rightarrow g = 0$

Example: Five lemma

Theorem (Five lemma)

Consider the following commutative diagram with exact rows in an abelian category.

If α is an epimorphism, β, δ are isomorphisms and ε is a monomorphism, then γ is an isomorphism.

$$\begin{array}{ccccccccc}
A & \xrightarrow{a} & B & \xrightarrow{b} & C & \xrightarrow{c} & D & \xrightarrow{d} & E \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\
A' & \xrightarrow[a']{} & B' & \xrightarrow[b']{} & C' & \xrightarrow[c']{} & D' & \xrightarrow[d']{} & E'
\end{array}$$

- f monomorphism iff $\forall g : fg = 0 \Rightarrow g = 0$
- f epimorphism iff $\forall g : gf = 0 \Rightarrow g = 0$, or equivalently $\forall g \, \exists h, e :$ codomain$(f) =$ codomain$(g) \Rightarrow fh = ge$ with e epi

Example: Five lemma

Theorem (Five lemma)

Consider the following commutative diagram with exact rows in an abelian category.

If α is an epimorphism, β, δ are isomorphisms and ε is a monomorphism, then γ is an isomorphism.

$$\begin{array}{ccccccccc} A & \xrightarrow{a} & B & \xrightarrow{b} & C & \xrightarrow{c} & D & \xrightarrow{d} & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ A' & \xrightarrow[a']{} & B' & \xrightarrow[b']{} & C' & \xrightarrow[c']{} & D' & \xrightarrow[d']{} & E' \end{array}$$

- f monomorphism iff $\forall g : fg = 0 \Rightarrow g = 0$
- f epimorphism iff $\forall g : gf = 0 \Rightarrow g = 0$, or equivalently $\forall g \, \exists h, e : \text{codomain}(f) = \text{codomain}(g) \Rightarrow fh = ge$ with e epi

Demonstration in MATHEMATICA

Conclusion

Summary

- Framework + software for automated proofs of operator statements
  - Proofs rely on Gröbner bases and reduction to zero
- Illustrated on “real world” examples
- Integrate properties beyond simple identities
  - Cancellability assumptions, existential claims,...
  - Requires finding polynomials with special form in ideal (e.g. by eliminating variables, ideal intersections, ...)

Conclusion

Summary

- Framework + software for automated proofs of operator statements
  - Proofs rely on Gröbner bases and reduction to zero
- Illustrated on "real world" examples
- Integrate properties beyond simple identities
  - Cancellability assumptions, existential claims,...
  - Requires finding polynomials with special form in ideal (e.g. by eliminating variables, ideal intersections, ...)

Outlook

- Integration of further inference steps + theoretical foundation
- Find further areas of application