Computing elements of certain form in ideals to prove properties of operators
- additional material

This Mathematica notebook accompanies the paper "*Computing elements of certain form in ideals to prove properties of operators*" by Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. In this notebook, we provide automated proofs of the operator statements discussed in the paper.

In order to run this notebook, make sure that the **OperatorGB** package is in the same folder as this notebook. Then, you can run the following commands.

In[1]:=
```
(* Loading the package *)
SetDirectory[NotebookDirectory[]];
<< OperatorGB.m
```

```
Package OperatorGB version 1.4.2
Copyright 2019, Institute of Mathematics, University of Kassel
by Clemens Hofstadler, clemens.hofstadler@mathematik.uni-kassel.de
```

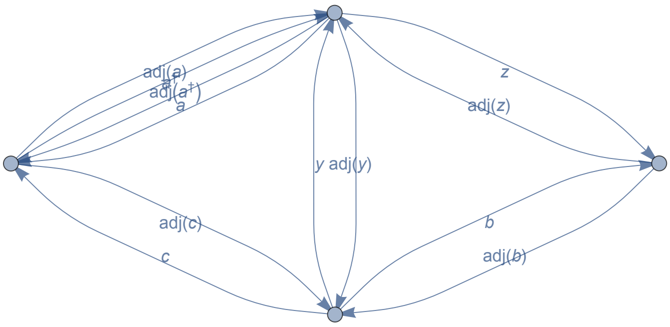
Theorem 1.1

Let $A : \mathcal{H}_4 \to \mathcal{H}_2$, $B : \mathcal{H}_1 \to \mathcal{H}_3$, $C : \mathcal{H}_1 \to \mathcal{H}_2$ be bounded linear operators on complex Hilbert spaces. There exists a bounded linear operator $X : \mathcal{H}_3 \to \mathcal{H}_4$ such that $A X B = C$ if and only if $\mathcal{R}(C) \subseteq \mathcal{R}(A)$ and $\mathcal{R}((A^\dagger C)^*) \subseteq \mathcal{R}(B^*)$.

The quiver Q encoding the domains and codomains of the operators involved consists of the four vertices $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4$ and a total of 12 edges representing the 12 indeterminates. Note that we also have to introduce variables for $A^\dagger$ and all adjoint operators as we also have to encode the properties of these operators.

In[3]:=
```
Q = {{a, H4, H2}, {adj[a], H2, H4}, {a†, H2, H4}, {adj[a†], H4, H2},
   {b, H1, H3}, {adj[b], H3, H1}, {c, H1, H2}, {adj[c], H2, H1},
   {y, H1, H4}, {adj[y], H4, H1}, {z, H4, H3}, {adj[z], H3, H4}};
PlotQuiver[
 Q]
```

Out[4]=



The following command defines the ring of noncommutative polynomials in the variables given by the labels of the quiver Q over the coefficient field $\mathbb{Q}$.

In[6]:=
```
SetUpRing[Q[[All, 1]]]
```

Sufficiency of the range conditions

The range inclusions appearing in the theorem above can be translated into the existence of operators Y and Z such that $C = A\,Y$ and $\left(A^{\dagger}\,C\right)^{*} = B^{*}\,Z$. Hence, we can translate the range inclusions into the following set of noncommutative polynomials.

In[7]:=
```
F = {c - a ** y, adj[a† ** c] - adj[b] ** z};
```

We have to add to this set of assumptions the polynomials representing the properties of $A^{\dagger}$, and all the respective adjoint statements.

In[8]:=
```
F = Join[F, Pinv[a]] // AddAdj;
```

To find a solution of the equation $A\,X\,B = C$, we intersect the two-sided ideal generated by F representing our assumptions with the right ideal J_{ρ} generated by a and c and check whether a Gröbner basis of this intersection contains an element of the form $a\,x\,b - c$ for some x.

In[9]:=
```
Jρ = {a, c};
int = IntersectRightIdeal[F, Jρ, Q, MaxDeg → 2];
solution = Cases[int, -c + a ** __ ** b]
```

Out[11]=
```
{-c + a ** adj[z] ** b}
```

We could indeed find a polynomial of the desired form. To finish the proof, we check that it is compatible with Q.

In[12]:=
```
CompatibleQ[-c + a ** adj[z] ** b, Q]
```

Out[12]=
```
True
```

Necessity of the range conditions

For this implication, our assumptions consist of the existence of a solution X to $A\,X\,B = C$, the defining identities of $A^\dagger$, and all the respective adjoint statements. This gives rise to the following set of polynomials.

```
In[13]:= F = Join[{a ** x ** b - c}, Pinv[a]] // AddAdj;
```

For this part of the proof, we have to extend the quiver in order to also include the variable x and its adjoint x^*.

```
In[14]:= Q = Join[Q, {{x, H3, H4}, {adj[x], H4, H3}}];
```

To prove the range inclusions, we have to find compatible polynomials in the ideal (F) representing the identities $C = A\,Y$ and $(A^\dagger\,C)^* = B^*\,Z$ where Y, Z are still unknown. We search for such elements by intersecting (F) with the right ideal J_ρ generated by a and c, respectively with the right ideal generated by $(a^\dagger\,c)^*$and b^*.

```
In[15]:= Jρ = {a, c};
int1 = IntersectRightIdeal[F, Jρ, Q, MaxDeg → 2];
rangeInclusion1 = Cases[int1, -c + a ** __]

Jρ = {adj[a† ** c], adj[b]};
int2 = IntersectRightIdeal[F, Jρ, Q, MaxDeg → 2];
rangeInclusion2 = Cases[int2, -adj[a† ** c] + adj[b] ** __]

Out[17]= {-c + a ** x ** b, -c + a ** a† ** c}

Out[20]= {-adj[c] ** adj[a†] + adj[b] ** adj[x] ** adj[a] ** adj[a†]}
```

We could indeed find polynomials of the desired form. To finish the proof, we check that they are compatible with Q.

```
In[21]:= CompatibleQ[#, Q] & /@ Join[rangeInclusion1, rangeInclusion2]

Out[21]= {True, True, True}
```

Theorem 1.2

Let $A : \mathcal{H}_3 \to \mathcal{H}_2,\ B : \mathcal{H}_1 \to \mathcal{H}_3,\ C : \mathcal{H}_1 \to \mathcal{H}_2$ be bounded linear operators on complex Hilbert spaces such that $\mathcal{R}(B) \subseteq \mathcal{R}(A^*)$. If there exists a bounded, positive linear operator $X : \mathcal{H}_3 \to \mathcal{H}_3$ such that $A\,X\,B = C$, then $B^*\,A^\dagger\,C$ is positive.

Here, our assumptions consist of the existence of a positive solution X to $A\,X\,B = C$ and of the range inclusion $\mathcal{R}(B) \subseteq \mathcal{R}(A^*)$, which we encode by the identities $A\,Y^*\,Y\,B = C$ and $B = A^*\,Z$, respectively, with new operators Y, Z.
Finally, we also have to add the defining identities of $A^\dagger$ and all the respective adjoint statements. This gives rise to the following set of polynomials.

```
In[22]:= F = Join[{a ** adj[y] ** y ** b - c, b - adj[a] ** z}, Pinv[a]] // AddAdj;
```

To use the procedure for computing the homogeneous part of an ideal, we have to add the identity $v - b^*\,a^\dagger\,c$ to our assumptions.

```
In[23]:= F = Join[F, {v - adj[b] ** a† ** c}];
```

The quiver Q encoding the domains and codomains of the operators involved consists of the three vertices $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ and a total of 12 edges representing the 12 indeterminates.

In[24]:=
```
Q = {{a, H3, H2}, {adj[a], H2, H3}, {a†, H2, H3}, {adj[a†], H3, H2},
   {b, H1, H3}, {adj[b], H3, H1}, {c, H1, H2}, {adj[c], H2, H1},
   {y, H3, H3}, {adj[y], H3, H3}, {z, H1, H2}, {adj[z], H2, H1}};
```

Next, we define the ring of noncommutative polynomials in the variables given by the labels of the quiver *Q* over the coefficient field ℚ and specify the degree matrix *A* w.r.t. which the homogeneous part will be computed.

In[26]:=
```
SetUpRing[Join[Q[[All, 1]], {v}]]
(* Setting up the degree matrix *)
A = Table[0, {i, WordOrder // Length}, {j, 6}];
A[[1, 1]] = 1; A[[2, 1]] = -1;
A[[3, 2]] = 1; A[[4, 2]] = -1;
A[[5, 3]] = 1; A[[6, 3]] = -1;
A[[7, 4]] = 1; A[[8, 4]] = -1;
A[[9, 5]] = 1; A[[10, 5]] = -1;
A[[11, 6]] = 1;
A[[12, 6]] = -1;
```

Before we proceed to compute the homogeneous part of (*F*), we first compute the reduced Gröbner basis of this ideal. This step is not necessary for the correctness of the procedure but it speeds up the computation. We then use this Gröbner basis, the degree matrix *A* and a termination criterion as input to enumerate a Gröbner basis of the homogeneous part of (*F*).

In[34]:=
```
G = Groebner[cofactors, F];
G = Interreduce[G][[1]];
(* Computing homA(I) *)
VerboseOperatorGB = 1;
hom = Hom[cofactors, G, 2, A];
```

```
G has 701 elements in the beginning.

Starting iteration 1...
8831 ambiguities in total
Iteration 1 finished. G has now 1450 elements

Starting iteration 2...
41555 ambiguities in total
Iteration 2 finished. G has now 11478 elements

Rewriting the cofactors...
```

We can see below that this Gröbner basis contains a polynomial of the desired form. Finally, we have to check that this polynomial (where the auxiliary variable *v* has been replaced by $b^* a^\dagger c$) is compatible with the quiver *Q*.

In[38]:=
```
hom[[27]]
CompatibleQ[adj[b] ** a† ** c - adj[b] ** adj[y] ** y ** b, Q]
```
Out[38]=
```
-v + adj[b] ** adj[y] ** y ** b
```
Out[39]=
```
True
```

Additional material: proofs of [1] that can be computer-supported now

In this section, we give more details on the very last point made in Section 3 of the paper. In particular, we discuss how ideal intersections can be used to support the proofs done in [1]. To exemplify this, we look at the implication (*i*) ⇒ (*v*) from the following theorem [1, Theorem 2.1].

Let A, B, C be complex matrices with Moore-Penrose inverses $A^\dagger$, $B^\dagger$, $C^\dagger$ such that $M = A\,B\,C$ is defined. Let $P = A^\dagger A\,B\,C\,C^\dagger$ and $Q = C\,C^\dagger B^\dagger A^\dagger A$. Then, the following are equivalent:
(i) $M^\dagger = C^\dagger B^\dagger A^\dagger$;
(ii) $Q \in P\{1, 2\}$ and both of $A^* A\,P\,Q$ and $Q\,P\,C\,C^*$ are Hermitian;
(iii) $Q \in P\{1, 2\}$ and both of $A^* A\,P\,Q$ and $Q\,P\,C\,C^*$ are EP;
(iv) $Q \in P\{1\}$, $\mathcal{R}(A^* A\,P) = \mathcal{R}(Q^*)$, and $\mathcal{R}(C\,C^* P^*) = \mathcal{R}(Q)$;
(v) $P\,Q = (P\,Q)^2$, $\mathcal{R}(A^* A\,P) = \mathcal{R}(Q^*)$, and $\mathcal{R}(C\,C^* P^*) = \mathcal{R}(Q)$;

[1] Cvetković-Ilić, D. S., Hofstadler, C., Hossein Poor, J., Milošević, J., Raab, C. G., and Regensburger, G., *Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law.* Appl. Math. Comput. **409**, Article 126357, 10 pages, 2021.

The assumptions of the implication (*i*) ⇒ (*v*) can be encoded by the following set of polynomials.

In[40]:=
```
F = Join[Pinv[a], Pinv[b], Pinv[c], Pinv[a ** b ** c, c† ** b† ** a†]] // AddAdj;
```

The following quiver encodes the domains and codomains of the theorem.

In[41]:=
```
QQ = {{a, H3, H4}, {adj[a], H4, H3}, {a†, H4, H3}, {adj[a†], H3, H4},
      {b, H2, H3}, {adj[b], H3, H2}, {b†, H3, H2}, {adj[b†], H2, H3},
      {c, H1, H2}, {adj[c], H2, H1}, {c†, H2, H1}, {adj[c†], H1, H2}};
```

In[42]:=
```
SetUpRing[QQ[[All, 1]]]
```

Proving the first assertion $P\,Q = (P\,Q)^2$ comes down to simply verifying ideal membership of an explicitly given polynomial. This could also be done automatically before. The following command *Certify* automatically applies the framework for algebraic proofs of operator statements, and in this way, automatically proves this assertion.

In[43]:=
```
p = a† ** a ** b ** c ** c†;
q = c ** c† ** b† ** a† ** a;
VerboseOperatorGB = 0;
certificate = Certify[F, p ** q ** p ** q - p ** q, QQ];
```
```
Done! All claims were successfully reduced to 0.
```

The two claimed range inclusions $\mathcal{R}(A^* A\,P) = \mathcal{R}(Q^*)$, and $\mathcal{R}(C\,C^* P^*) = \mathcal{R}(Q)$ can be translated into the existence of operators U_1, U_2, V_1, V_2 such that

$$A^* A\,P = Q^* V_1, \qquad A^* A\,P\,V_2 = Q^*, \qquad C\,C^* P^* = Q\,U_1,$$

$C\,C^*\,P^*\,U_2 = Q$.

In [1], the following was noted: "*By inspecting the proof of Theorem 2.3 one can see that these can be chosen as*

$$V_1 = B^* A^* A B C C^\dagger, \qquad V_2 = B^\dagger A^\dagger (A^\dagger)^* (B^\dagger)^* (C^\dagger)^* C^*, \quad U_1 = B C C^* B^* A^* (A^\dagger)^*,$$

$U_2 = (B^\dagger)^* (C^\dagger)^* C^\dagger B^\dagger A^\dagger A$."

Now, using the methods for intersecting ideals, we can find the polynomials that represent these operators automatically.

To this end, we intersect the two-sided ideal (F) generated by our assumptions F, with the right ideal generated by $a^*\,a\,p$ and q^* to obtain V_1 and V_2, respectively with the right ideal generated by $c\,c^*\,p^*$ and q to obtain U_1 and U_2.

In[47]:=
```
(* find V1 *)
SetUpRing[QQ[[All, 1]] // Reverse];
Jρ = {adj[a] ** a ** p, adj[q]};
R1 = IntersectRightIdeal[F, Jρ, QQ, MaxDeg → 2];
R1 = Cases[R1, -adj[a] ** a ** p + adj[q] ** ___][[1]];
(* find V2 *)
SetUpRing[QQ[[All, 1]]];
R2 = IntersectRightIdeal[F, Jρ, QQ, MaxDeg → 2];
R2 = Cases[R2, -adj[q] + adj[a] ** a ** p ** ___][[1]];
(* find U1 *)
SetUpRing[QQ[[All, 1]] // Reverse];
Jρ = {c ** adj[c] ** adj[p], q};
R3 = IntersectRightIdeal[F, Jρ, QQ, MaxDeg → 2];
R3 = Cases[R3, -c ** adj[c] ** adj[p] + q ** ___][[1]];
(* find U2 *)
SetUpRing[QQ[[All, 1]]];
R4 = IntersectRightIdeal[F, Jρ, QQ, MaxDeg → 2];
R4 = Cases[R4, -q + c ** adj[c] ** adj[p] ** ___][[1]];
```

In the following, we pretty-print the found polynomials. One can observe that these polynomials lead to the same U_1, U_2, V_1, V_2 that were also used in [1].

In[61]:=
```
R1 /. {p → "p", q → "q", adj[p] → adj["p"], adj[q] → adj["q"]}
R2 /. {p → "p", q → "q", adj[p] → adj["p"], adj[q] → adj["q"]}
R3 /. {p → "p", q → "q", adj[p] → adj["p"], adj[q] → adj["q"]}
R4 /. {p → "p", q → "q", adj[p] → adj["p"], adj[q] → adj["q"]}
```

Out[61]= `-adj[a] ** a ** p + adj[q] ** adj[b] ** adj[a] ** a ** b ** c ** c†`

Out[62]= `-adj[q] + adj[a] ** a ** p ** b† ** a† ** adj[a†] ** adj[b†] ** adj[c†] ** adj[c]`

Out[63]= `-c ** adj[c] ** adj[p] + q ** b ** c ** adj[c] ** adj[b] ** adj[a] ** adj[a†]`

Out[64]= `-q + c ** adj[c] ** adj[p] ** adj[b†] ** adj[c†] ** c† ** b† ** a† ** a`

To finish the proof, we check that these polynomials are indeed compatible with the quiver.

In[66]:=
```
CompatibleQ[#, QQ] & /@ {R1, R2, R3, R4}
```

Out[66]= `{True, True, True, True}`