UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 15

Splitting Algorithm for vector bundles

by

B. Martin and T. Siebert

September 1997

The Zentrum für Computeralgebra (Centre for Computer Algebra) at the University of Kaiserslautern was founded in June 1993 by the Ministerium für Wissenschaft und Weiterbildung in Rheinland-Pfalz (Ministry of Science and Education of the state of Rheinland-Pfalz). The centre is a scientific institution of the departments of **Mathematics, Computer Science, and Electrical Engineering** at the University of Kaiserslautern.
The goals of the centre are to advance and to support the use of Computer Algebra in industry, research, and teaching. More concrete goals of the centre include

- the development, integration, and use of software for Computer Algebra
- the development of curricula in Computer Algebra under special consideration of interdisciplinary aspects
- the realisation of seminars about Computer Algebra
- the cooperation with other centres and institutions which have similar goals

The present coordinator of the Reports on Computer Algebra is:
Olaf Bachmann (email: `obachman@mathematik.uni-kl.de`)

Zentrum für Computeralgebra
c/o Prof. Dr. G.-M. Greuel, FB Mathematik
Erwin-Schrödinger-Strasse
D-67663 Kaiserslautern; Germany
Phone: 49 - 631/205-2850 Fax: 49 - 631/205-5052
email: `greuel@mathematik.uni-kl.de`
URL: `http://www.mathematik.uni-kl.de/~zca/`

Splitting algorithm for vector bundles

Bernd Martin, Thomas Siebert
Brandenburgische Technische Universität Cottbus
Institut für Mathematik
PF 101344 03046 Cottbus
martin@math.tu-cottbus.de

September 28, 1997

Abstract

A new criteria for indecomposability of vector bundles on projective varieties is presented. It is deduced from a new finite algorithm computing direct sum decompositions of graded modules over graded algebras. This algorithm applies as well to modules over local complete algebras over a field.

1 Introduction and notation

Let $(R, \underline{m})$ be either a complete local Noetherian commutative algebra over a field K or a graded K-algebra $R = \oplus_{d \leq 0} R_d$, $R_0 = K$ and $\underline{m} = \oplus_{d>0} R_d$. Let $M \in \operatorname{Mod} R$ be a finitely generated (or graded resp.) R-module. In the local case it is known (cf. [Yo]) that the module M is indecomposable if and only if the endomorphism ring $\operatorname{End}(M)$ is local. But this criteria is difficult to handle, since it involves usage of non–commutative methods. Here we present several versions of a criteria based on a presentation matrix of M, which may be checked using only the Groebner–basis algorithm in various forms. The algorithm has several applications:

- (i_1) Let R be the graded coordinate ring of a projective K-variety $X = Proj\ R$, let V be a vector bundle on X with $M \in \operatorname{Mod} R$ an associated graded R-module. The algorithm produces the direct sum decomposition of V.

- (i_2) More general, let $\mathcal{M}$ be a coherent sheaf on X. We can decide wether $\mathcal{M}$ is indecomposable.

- (i_3) Let R be the local ring of an isolated hypersurface singularity X defined by a polynomial equation $f(x_1, \ldots, x_n)$. If X is a suspension over X_0, i.e. $f = f_0(x_1, \ldots, x_{n-1}) + x_n^t$ and f_0 an equation of X_0, there is a useful theorem (cf. [HP] (2.8)) connecting maximal Cohen-Macaulay-modules (MCM) over X and X_0 and generalizing Knörrer's periodicity theorem.

  THEOREM *If $M \in MCM(X)$ and $R_i := R/x_n^{i+1}R$, $M_i := M \otimes R_i$ then $syz_R(M_{t-2}) \cong M \oplus syz_R(M)$ and M_{t-2} is a deformation of M_0 over R_{t-2}.*

  Knowing $M_0 \in MCM(X_0)$ we obtain MCM's over R by computing infinitesimal deformations of M_0 and then inspecting the direct summands of their R-syzygy-module. In this way computations are partially done for X_0 an A_k-singularity (cf. [MPP]), which has stimulated the development of the algorithm. Our algorithm is used for the verification of the indecomposability of the module constructed there.

Throughout this paper we restrict the notation to the local case. The graded case is handled analogously.

First we will fix some notation. A module M may be presented by matrices $Q \in \mathrm{Mat}(r,n;R)$, $M \cong \mathrm{coker}\,(Q)$. For simplicity we shall assume that r is always the number $l(M/\underline{m}M)$ of generators of M. On the other hand, n may be any integer, provided that it is at least equal to the number of generators of the syzygy module $syz\,(M)$, and may change during our considerations. All presentation matrices M of fixed size form an orbit under the obvious **RL**-action of $Gl_r(R)\times Gl_n(R)$ on Mat $(r,n;R)$.
We simply call two matrices with r rows (right)-**equivalent** if their columns generate the same submodule of R^r:

$$Q \sim Q' \Longleftrightarrow \langle Q\rangle = \langle Q'\rangle \subseteq R^r \Longleftrightarrow Q = Q'V' \quad \text{and} \quad Q' = QV$$

for some matrices V and V'. The change to another equivalent matrix corresponds to taking another basis of the module $\langle Q\rangle$. If Q and Q' have the same number n of columns, then $V' = V^{-1} \in Gl_n(R)$ is necessarily regular.
Multiplying Q from the left by a regular matrix corresponds to row operations, which change $\langle Q\rangle$. In general, it induces an isomorphism on coker(Q). We observe that $M = M_1 \bigoplus M_2$ is decomposable if and only if there exists a presentation matrix Q_0 of M in diagonal block form

$$Q_0 = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \quad \mathrm{coker}\,(A) \cong M_1,\ \mathrm{coker}\,(D) \cong M_2,$$

or, equivalently, there exists a regular matrix $U \in Gl_r(R)$, such that $Q \sim UQ_0$ for any presentation matrix Q of M. In the following, Q_0 always denotes a block diagonal matrix as above.

2 Block type Bruhat decomposition

For the convenience of the reader, we include some elementary, well-known facts from linear algebra which we shall need.
(2.1) Fix an integer $k \in \{1,\ldots,r-1\}$ and let

$$\mathbb{G} = \mathbb{G}_{(k)} = \left\{ \begin{pmatrix} S & T \\ V & W \end{pmatrix} \in Gl_r(R) \;\middle|\; S \in Gl_k(R),\ W \in Gl_{r-k}(R) \right\}.$$

After a permutation of rows (or columns), any regular matrix will belong to $\mathbb{G}$.
Consider the following subgroups of Gl_r contained in $\mathbb{G}$:

$$\begin{aligned} \mathbb{D} = \mathbb{D}^{(k)} &= \left\{ \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix} \in \mathbb{G} \right\}, \\ \mathbb{B}_+ = \mathbb{B}_+^{(k)} &= \left\{ \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \middle| T \in \mathrm{Mat}\,(k, r-k) \right\}, \\ \mathbb{B}_- = \mathbb{B}_-^{(k)} &= \left\{ \begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \middle| V \in \mathrm{Mat}\,(r-k, k) \right\}, \end{aligned}$$

where I always denotes the unit matrix of the corresponding size.
(2.2) The following lema will be verified by direct computation:

Lemma 1
Using the notation above,

(i1) $\mathbb{D} \subseteq \mathrm{N}(\mathbb{B}_+) \cap \mathrm{N}(\mathbb{B}_-)$,
(i2) $\mathbb{G} = \mathbb{G}^{-1}$,
(i3) $\mathbb{G} \subseteq \mathbb{D}\cdot\mathbb{B}_+\cdot\mathbb{B}_- \cap \mathbb{D}\cdot\mathbb{B}_+\cdot\mathbb{B}_-$.

Here $N(\ )$ denotes the normalizer in $Gl_r(R)$.
(i1) Just check the following identities:

$$\begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix} \cdot \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & STW^{-1} \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix} \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ V & I \end{pmatrix}$$

$$= \begin{pmatrix} I & 0 \\ WVS^{-1} & I \end{pmatrix} \cdot \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix}$$

(i2) From the identity

$$\begin{pmatrix} S & T \\ V & W \end{pmatrix} \cdot \begin{pmatrix} S' & T' \\ V' & W' \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix},$$

assuming that the first matrix is in $\mathbb{G}$, we obtain $T' = -S^{-1}TW'$ and $V' = -W^{-1}VS'$; hence, $SS' - TW^{-1}VS' = I$. Thus, S' is invertible and $\tilde{S} := S - TW^{-1}V$ is its inverse. Similarly, $\tilde{W} := W - VS^{-1}T$ is the inverse of W' .
(i3) Using the notation of *(i2)* we obtain

$$\begin{aligned} \begin{pmatrix} S & T \\ V & W \end{pmatrix} &= \begin{pmatrix} \tilde{S} & 0 \\ 0 & W \end{pmatrix} \cdot \begin{pmatrix} I & S'T \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ W^{-1}V & I \end{pmatrix} \\ &= \begin{pmatrix} S & 0 \\ 0 & \tilde{W} \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ W'V & I \end{pmatrix} \cdot \begin{pmatrix} I & S^{-1}T \\ 0 & I \end{pmatrix}. \end{aligned}$$

(2.3) Fix a k-subset J of row indices $\{1, ..., r\}$. Let Q_J be the submatrix of Q formed by those rows of Q whose index belongs to J. Then $\mathcal{M}_J(Q) := \langle Q_J \rangle \subseteq R^k$ is invariant under equivalence of matrices. After a certain permutation of rows of Q, it is enough to consider for simplicity only the special cases $J_0 = \{1, ..., k\}$, $J_0' = \{k+1, ..., r\}$. To simplify the notation, set $\mathcal{M}(Q) := \mathcal{M}_{J_0}(Q)$, $\mathcal{M}'(Q) := \mathcal{M}_{J_0'}(Q)$.

Lemma 2
If $Q \sim UQ_0$, $U \in \mathbb{B}_+$, then $\mathcal{M}(Q_0) \subseteq \mathcal{M}(Q)$ and $\mathcal{M}'(Q_0) = \mathcal{M}'(Q)$.

In other words, under this assumtion the set $\{\mathcal{M}(UQ) \mid U \in \mathbb{B}_+\}$ of submodules of R^k contains an absolute minimal element.

$$Q = \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} A & TD \\ 0 & D \end{pmatrix},$$

hence

$$\mathcal{M}(Q) = \langle A \rangle + \langle TD \rangle \supseteq \langle A \rangle = \mathcal{M}(Q_0) \text{ and } \mathcal{M}'(Q) = \langle D \rangle = \mathcal{M}'(Q_0).$$

3 Row-minimal matrices

(3.1) In virtue of Lemma 2 we shall look for presentation matrices which have a good chance of being equivalent to a matrix in block diagonal form.

Definition 3
For a given $J \subset \{1, ..., r\}$ we call Q a **J-row-minimal** *matrix if $\mathcal{M}(P_\sigma Q)$ is minimal in the set of R^k-submodules $\{\mathcal{M}(UP_\sigma Q) \mid U \in \mathbb{B}_+\}$, where P_σ is a permutation matrix such that the associated permutation σ maps J to J_0.*

Obviously, this notation is independent of the choice of σ. Moreover, Q is called **row-minimal** if it is J-row-minimal with respect to all strict subsets J of row indices $\{1, ..., r\}$.

(3.2) The test for whether a module M will split is based on the observation that a presentation matrix of M in block diagonal form Q_0 is J_0- and J_0'-row-minimal (cf. Lemma 2). It is possible to check by a standard basis computation whether a row-minimal matrix Q is equivalent to a block diagonal matrix. To do that, we have to fix an arbitrary (local) monomial order of R^r, ordering first by components; that is, $m\underline{e}_i > m'\underline{e}_j$ for any two monomials $m,\ m'$ and $i < j$, $\underline{e}_i$ the i-th unit column.

(3.3) Let $Q' \sim Q$ be a matrix formed by an ordered standard basis of $\langle Q\rangle$. From the above order we obtain an integer l such that all columns of Q' having index $l' > l$ will have their first non-zero entry in the k'-th component, $k' > k$. Hence Q' will have the block structure

$$Q' = \begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix}, \quad A' \in \mathrm{Mat}\,(k, l; R),$$

and the modules associated to A' and D' are characterized by Q:

$$\langle A'\rangle = \mathcal{M}(Q), \quad \langle D'\rangle = \left\{ \underline{y} \in R^{r-k} \,\middle|\, \begin{pmatrix} 0 \\ \underline{y} \end{pmatrix} \in \langle Q\rangle \right\}.$$

Changing the roles of J_0 and J_0' (resp. reversing the order of components) we may write a corresponding standard basis Q'' in analogous block form

$$Q'' = \begin{pmatrix} A'' & B'' \\ 0 & D'' \end{pmatrix}.$$

Comparing these two different standard bases of Q, we obtain as a trivial consequence

Lemma 4
With the notation from above

$$Q \sim Q_0 \quad \textit{if and only if} \quad \langle A'\rangle = \langle A''\rangle \quad \textit{and} \quad \langle D'\rangle = \langle D''\rangle.$$

(3.4) Usually we are not in this situation and we first have to apply row operations. But, assuming J_0-row-minimality, it is enough to apply only those row-operations belonging to $I\!B_+$:

Proposition 5
If $Q' \sim UQ_0$ for some $U \in G\!\!\!\!G$ and
if Q' is J_0-row-minimal, then

(i1) $\langle A'\rangle = \mathcal{M}(Q) \cong \mathcal{M}(Q_0) = \langle A\rangle$
(i2) $\binom{0}{\underline{y}} \in \langle Q\rangle \Longleftrightarrow \underline{y} \in \mathcal{M}'(Q_0)$*; that is,* $\langle D'\rangle = \langle D\rangle$.

(i0) First note that given an isomorphism $\varphi : R^l \to R^l$ and a φ^{-1}-invariant submodule $N \subset R^l$, then N is φ-invariant, too (otherwise $N \subset \varphi(N) \subset \varphi^2(N) \ldots$ would produce an infinite ascending chain!).
(i1) With the notation of (3.3) let

$$Q \sim Q' = \begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix} \sim \underbrace{\begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \cdot \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix}}_{U \in G\!\!\!\!G} \cdot \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}.$$

Letting $\tilde{A} := SA, \tilde{D} := WD$, $\tilde{I} := I + VT$, we obtain

$$\begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix} \sim \begin{pmatrix} I & T \\ V & \tilde{I} \end{pmatrix} \cdot \begin{pmatrix} \tilde{A} & 0 \\ 0 & \tilde{D} \end{pmatrix} = \begin{pmatrix} \tilde{A} & T\tilde{D} \\ V\tilde{A} & \tilde{I}\tilde{D} \end{pmatrix},$$

$\mathcal{M}(Q) = \langle A' \rangle = \langle \tilde{A} \rangle + \langle T\tilde{D} \rangle \supseteq \langle \tilde{A} \rangle \cong \langle A \rangle$. Because of the minimality assumption,

$$\langle \tilde{A} \rangle \subseteq \mathcal{M}(Q) \subseteq \mathcal{M}\left(\begin{pmatrix} I & -\tilde{T} \\ 0 & I \end{pmatrix} \cdot Q\right).$$

Again, by Lemma 1*(i3)*, we have a factorization

$$\begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \cdot \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & \tilde{T} \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ \tilde{V} & I \end{pmatrix} \cdot \begin{pmatrix} \tilde{S} & 0 \\ 0 & \tilde{W} \end{pmatrix}.$$

Consequently, we obtain

$$\mathcal{M}\left(\begin{pmatrix} I & -\tilde{T} \\ 0 & I \end{pmatrix} \cdot Q\right) = \mathcal{M}\left(\begin{pmatrix} I & 0 \\ \tilde{V} & I \end{pmatrix} \cdot \begin{pmatrix} \tilde{S} & 0 \\ 0 & \tilde{W} \end{pmatrix} \cdot \begin{pmatrix} \tilde{A} & 0 \\ 0 & \tilde{D} \end{pmatrix}\right) = \langle \tilde{S}\tilde{A} \rangle,$$

and, by the initial remark, $\langle \tilde{A} \rangle = \mathcal{M}(Q) = \langle \tilde{S}\tilde{A} \rangle$.
(i2) An easy computation shows that

$$\begin{aligned} \underline{y} \in \langle D' \rangle \quad &\Longleftrightarrow \quad \begin{pmatrix} \underline{0} \\ \underline{y} \end{pmatrix} \in \langle Q \rangle \\ &\Longleftrightarrow \quad \begin{pmatrix} \underline{0} \\ \underline{y} \end{pmatrix} \in \langle \begin{pmatrix} \tilde{A} & T\tilde{D} \\ V\tilde{A} & \tilde{I}\tilde{D} \end{pmatrix} \rangle \\ &\Longleftrightarrow \quad \begin{pmatrix} \underline{0} \\ \underline{y} \end{pmatrix} = \begin{pmatrix} \tilde{A} & T\tilde{D} \\ V\tilde{A} & \tilde{I}\tilde{D} \end{pmatrix} \cdot \begin{pmatrix} \underline{f} \\ \underline{g} \end{pmatrix} \\ &\Longleftrightarrow \quad \tilde{A}\underline{f} = -T\tilde{D}\underline{g} \text{ and } \underline{y} = V\tilde{A}\underline{f} + \tilde{I}\tilde{D}\underline{g}. \end{aligned}$$

Thus, $\underline{y} = (\tilde{I} - VT)\tilde{D}g = (I + VT - VT)\tilde{D}\underline{g} = \tilde{D}g$, which shows that $\langle D' \rangle \subseteq \langle \tilde{D} \rangle$. On the other hand $\underline{y} \in \langle \tilde{D} \rangle$ implies the existence of a $\underline{g}$ such that $\underline{y} = \tilde{D}\underline{g}$. Because $\langle T\tilde{D} \rangle \subseteq \langle A' \rangle = \langle A \rangle$, there is an $\underline{f}$ such that $-T\tilde{D}g = \tilde{A}\underline{f}$; that is, $\begin{pmatrix} \underline{0} \\ \underline{y} \end{pmatrix} \in \langle Q \rangle$ and $\underline{y} \in \langle D' \rangle$.

4 Splitting criteria

(4.1) Next we want to characterize those row-minimal matrices belonging to a decomposable module. The idea comes from the fact that the canonical homomorphism $R^r \longrightarrow R^k/\mathcal{M}(Q) \oplus R^{r-k}/\mathcal{M}'(Q)$ factors via M and that the induced surjection $M \longrightarrow R^k/\mathcal{M}(Q) \oplus R^{r-k}/\mathcal{M}'(Q)$ is an isomorphism. Hence, it reflects a direct sum decomposition of M if and only if Q is equivalent to a block diagonal matrix Q_0. Then Q is necessarily row-minimal with respect to J_0 and J_0'.

Proposition 6
If Q is row-minimal, then $M = \operatorname{coker} Q$ is decomposable if and only if for some permutation σ, $P_\sigma Q \sim Q_0$.

Assume M splits. Then we know $\tilde{U}Q \sim Q_0$ and, for some permutation σ, $\tilde{U}P_{\sigma^{-1}} \in \mathcal{G}$; i.e., $P_\sigma Q \sim UQ_0$ and $U = P_\sigma \tilde{U}^{-1} \in \mathcal{G}$. By Proposition 5*(i2)*, we obtain

$$\mathcal{M}'(P_\sigma Q) \supseteq \left\{ \underline{y} \in R^{r-k} \middle| \begin{pmatrix} \underline{0} \\ \underline{y} \end{pmatrix} \in \langle P_\sigma Q \rangle \right\} \cong \mathcal{M}'(Q_0).$$

The same holds for J_0' , because Q is J_0'-row-minimal, too; that is,

$$\mathcal{M}(P_\sigma Q) \supseteq \left\{ \underline{x} \in R^k \middle| \begin{pmatrix} \underline{x} \\ \underline{0} \end{pmatrix} \in \langle P_\sigma Q \rangle \right\} \cong \mathcal{M}(Q_0).$$

But then the composition of the canonical surjection

$$M \longrightarrow R^k/\mathcal{M}(P_\sigma Q) \oplus R^{r-k}/\mathcal{M}'(P_\sigma Q)$$

with

$$R^k/\mathcal{M}(P_\sigma Q) \oplus R^{r-k}/\mathcal{M}'(P_\sigma Q) \longrightarrow R^k/\mathcal{M}(Q_0) \oplus R^{r-k}/\mathcal{M}'(Q_0) \cong M$$

must be an isomorphism, showing $P_\sigma Q \sim Q_0$.
Note: $\mathcal{M}(P_\sigma Q)$ and $\mathcal{M}'(P_\sigma Q)$ are computed by a standard basis computation with respect to a certain module ordering in the components. So we simply have to check whether

$$P_\sigma Q = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \cdot X,\ A := \mathcal{M}(P_\sigma Q),\ D := \mathcal{M}'(P_\sigma Q)$$

has a solution X, which corresponds to a simple syzygy computation.
(4.2) Before computing a solution X, it is necessary for Q to be row-minimal, which may be tested using methods discussed in the next section. Usually Q is not row-minimal, in which case we shall use an algorithm to transform Q into an equivalent and J_0-row-minimal matrix. But we do not know a procedure to obtain row-minimality for all subsets immediately. Hence we shall formulate a second version of the splitting criteria.

Proposition 7
If Q is J_0-row-minimal, then

$$Q \sim UQ_0,\ U \in \mathbb{G} \qquad \textit{if and only if} \qquad Q \sim UQ_0,\ U \in \mathbb{B}_-.$$

By Proposition 5, it follows that

$$U = \begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \cdot \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} S & 0 \\ 0 & W \end{pmatrix} \text{ and } Q \sim Q' = \begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix},$$

then $\langle A' \rangle = \langle \tilde{A} \rangle,\ \tilde{A} := SA$ and $\langle D' \rangle = \langle \tilde{D} \rangle,\ \tilde{D} := WD$. Therefore

$$\begin{pmatrix} A' & 0 \\ C' - VA' & D' \end{pmatrix} = \begin{pmatrix} I & 0 \\ -V & I \end{pmatrix} Q' \sim \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} \tilde{A} & 0 \\ 0 & \tilde{D} \end{pmatrix} = \begin{pmatrix} \tilde{A} & T\tilde{D} \\ 0 & \tilde{D} \end{pmatrix}$$

and $\langle T\tilde{D} \rangle \subseteq \langle A' \rangle = \langle \tilde{A} \rangle$, giving

$$\begin{pmatrix} \tilde{A} & T\tilde{D} \\ 0 & \tilde{D} \end{pmatrix} \sim \begin{pmatrix} \tilde{A} & 0 \\ 0 & \tilde{D} \end{pmatrix} \sim \begin{pmatrix} A' & 0 \\ 0 & D' \end{pmatrix},$$

from which it may be concluded that

$$Q \sim \begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \cdot \begin{pmatrix} A' & 0 \\ 0 & D' \end{pmatrix}, \quad \begin{pmatrix} I & 0 \\ V & I \end{pmatrix} \in \mathbb{B}_-.$$

The other direction is obvious. Note:
$\begin{pmatrix} A' & 0 \\ C' - VA' & D' \end{pmatrix} \sim \begin{pmatrix} A' & 0 \\ 0 & D' \end{pmatrix}$ if and only if $C' - VA' = D'V'$ for some V'; i.e. we obtain

Corollary 8
If Q is J_0-row-minimal, then for an ordered standard basis $Q' = \begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix}$ of Q we have:
$Q \sim UQ_0,\ U \in \mathbb{G}$ *if and only if* *the equation $VA' + D'V' = C'$ has a solution (V, V').*

Deciding the solvability of the above equation is reduced to a lifting computation: Let A^* and D^* be matrices corresponding to Hom $(-, A')$ and Hom $(D', -)$, and let $[V]$, $[V']$, $[C']$ denote flattenings to a column vector of V, V', C', respectively. Then we obtain

$$(A^*\ D^*) \cdot \begin{pmatrix} [V] \\ [V'] \end{pmatrix} = [C'];$$

that is, $[C']$ can be lifted to $(A^*\ D^*)$ if and only if the equation has a solution.

5 Criteria for row-minimality

(5.1) Fix $J = J_0 = \{1, ..., k\}$. Consider all those matrices $U_T = \begin{pmatrix} I & T \\ 0 & I \end{pmatrix}$ from $\mathbb{B}_+$ which do not increase $\mathcal{M}(Q)$, $Q = \begin{pmatrix} Q_J \\ Q_{J'} \end{pmatrix}$, and set

$$\mathcal{N}_Q^{(J)} := \{T \in \mathrm{Mat}(k, r-k; R) \mid \mathcal{M}(U_T Q) \subseteq \mathcal{M}(Q)\}.$$

Because $U_T Q = \begin{pmatrix} Q_J + TQ_{J'} \\ Q_{J'} \end{pmatrix}$ and $\mathcal{M}(U_T Q) = \langle Q_J + TQ_{J'} \rangle \subseteq \mathcal{M}(Q) = \langle Q_J \rangle$ if and only if $\langle TQ_{J'} \rangle \subseteq \langle Q_J \rangle$, we obtain:

$$\mathcal{N}_Q^{(J)} = \{T \in \mathrm{Mat}(k, r-k; R) \;\mid\; \text{there exists } \tilde{T} \in \mathrm{Mat}(n, n; R): \; TQ_{J'} - Q_J \tilde{T} = 0\}.$$

Choose a basis $T_1, \ldots, T_N$ of the module $\mathcal{N}_Q^{(J)}$ and a set of associated matrices $\tilde{T}_1, \ldots, \tilde{T}_N \in \mathrm{Mat}(n, n; R)$.

Proposition 9 *(sufficient condition for J-row-minimality)*
Q is J-row-minimal if either

(i1) $\tilde{T}_1, \ldots, \tilde{T}_N$ do not have a unit entry; i.e., $\tilde{T}_i \bmod \underline{m} = 0$
or
(i2) for any $T \in \mathcal{N}_Q^{(J)}$, the corresponding matrix $\tilde{T}$ satisfies the condition: $\tilde{T} \bmod \underline{m}$ is nilpotent.

Condition *(i1)* implies *(i2)*. Assuming *(i2)*, we obtain for any $T \in \mathcal{N}_Q^{(J)}$

$$\begin{aligned} \mathcal{M}(U_T Q) &= \langle Q_J + TQ_{J'} \rangle = \langle Q_J + Q_J \tilde{T} \rangle \\ &= \langle Q_J (I + \tilde{T}) \rangle = \langle Q_J \rangle = \mathcal{M}(Q), \end{aligned}$$

because $I + \tilde{T}$ is invertible. Therefore Q is J-row-minimal.

(5.2) In order to obtain a necessary condition for row-minimality, we have to improve the choice of a good representative $\tilde{Q}$ in the equivalence class of Q, cf. (3.3). Write $\tilde{Q}$ in block form

$$\tilde{Q} = \begin{pmatrix} A & 0 \\ C & D \end{pmatrix}, \qquad A \in \mathrm{Mat}(k, l).$$

We may assume that the columns of A form a completely reduced, minimal basis of $\mathcal{M}(Q)$. This means the columns of A form a minimal system of generators, increasingly ordered, and the l-th generator is reduced with respect to the standard basis generated by the first $l-1$ generators for appropriate l.

Lemma 10 *Let Q be a submodule of R^k, given by a completely reduced, minimal basis $A = (\underline{a}_1, \ldots, \underline{a}_r)$. A submodule P of Q is proper if and only if $lead(P)$, the initial module, does not contain all leading terms of A.*

We want to show that for a proper submodule P the minimal leading term not contained in $lead(Q)$ must be in $lead(A)$. Assume the contrary; i.e. the minimal $lead(\underline{q}_*) = q\underline{e}_l \notin P$ is not contained in $lead(A)$. We introduce the module $S = \langle m\underline{e}_s | m\underline{e}_s > q\underline{e}_l \rangle$, generated by all monomials in R^k which are greater than $q\underline{e}_l$.
Considering the whole situation in the factor module R^n/S, we have the equation

$$q\underline{e}_l = \sum_i g_i \underline{a}_i,$$

and, from the assumption on reducedness, it follows that all g_i belong to the maximal ideal $\underline{m}$. The staircases of both modules Q and P are identical up to $q\underline{e}_l$, and, hence, for every generator $\underline{a}_i$ an equation

$$\underline{a}_i = \sum_k h_{ik}\underline{p}_k + c_i q\underline{e}_l$$

with $c_i \in K$ exists. We obtain

$$q\underline{e}_l = \sum_{i,k} g_i h_{ik}\underline{p}_k + \sum_i g_i c_i q\underline{e}_l.$$

The second summand vanishes in R^n/S. Thus, $q\underline{e}_l$ must be a leading term of P, too.
The other implication is a well–known fact about standard basis.

(5.3) Without loss of generality we will assume that $Q = \tilde{Q} = \begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$ fulfills the conditions of (5.2). For $T \in \mathcal{N}_Q^{(J)}$ we obtain $U_T Q = \begin{pmatrix} A+TC & TD \\ C & D \end{pmatrix}$ and $\langle TC\rangle + \langle TD\rangle \subseteq \langle A\rangle$. Therefore, matrices $\tilde{T}' \in \mathrm{Mat}(l,l;R)$ and $\tilde{T}'' \in \mathrm{Mat}(l,n-l;R)$ do exist such that $TC = A\tilde{T}'$ and $TD = A\tilde{T}''$. In the notation of (5.1), $\tilde{T} = \begin{pmatrix} \tilde{T}' & \tilde{T}" \\ 0 & 0 \end{pmatrix}$ holds. Define associated constant matrices $\tilde{T}_0' := \tilde{T}' \bmod \underline{m}$ and $\tilde{T}_0'' := \tilde{T}'' \bmod \underline{m}$.

Proposition 11 *(necessary condition for J-row-minimality)*
Using the above notation, for any $T \in \mathcal{N}_Q^{(J)}$ the associated constant (l,n)-matrix $\left(I + \tilde{T}_0', \tilde{T}_0''\right)$ has full rank l if Q is J-row-minimal.

Note that $\tilde{T}_0'$ nilpotent implies the rank-condition.
By assumption (5.2), the columns of A induce an $(R/\underline{m})$-basis of $\langle A/\underline{m}A\rangle$. If $\left(I + \tilde{T}_0',\ \tilde{T}_0''\right)$ does not have full rank l, then $\langle A\left(I + \tilde{T}_0',\ \tilde{T}_0''\right)\rangle + \underline{m}\langle A\rangle \subset \langle A\rangle$ is a strict submodule. Hence, by lemma of Nakayama, $\mathcal{M}(U_T Q) = \langle A(I + \tilde{T}', \tilde{T}'')\rangle$ is a strict submodule of $\langle A\rangle$, too, and Q is not J-row-minimal!

6 Finding a J-row-reduction

(6.1) In looking for a strict J-row-reduction of a presentation matrix Q, we have to find a matrix T from $\mathcal{N}_Q^{(J)}$ such that for the associated constant matrix

$$N = N_T := \left(\tilde{T}_0', \tilde{T}_0''\right) \in \mathrm{Mat}\ (l, n; R/\underline{m}) : \quad \mathrm{rk}\left(\tilde{I} + N\right) < l;$$

here $\tilde{I} := (I_l, 0)$. The set $\left\{N_T | T \in \mathcal{N}_Q^{(J)}\right\}$ forms a linear subspace of $\mathrm{Mat}\,(l, n; R/\underline{m})$. Choose a basis $N_1, \ldots, N_q$ and consider the generic matrix

$$N_* = N_*(Z) := \tilde{I} + \sum_{i=1}^{q} N_i \cdot Z_i.$$

Finding a reduction is equivalent to obtaining a zero $\underline{z}$ of the ideal of maximal minors

$$minor(N_*) \subset K[Z_1, ..., Z_q],$$

which, in general, seems to be not possible. (For simplicity we assume $K = R/\underline{m}$.)

(6.2) If our presentation matrix Q splits with respect to J, then by Lemma 2 there exists a unique minimal module $\langle A_0\rangle$ in $\{\mathcal{M}(U_TQ)|T \in \mathcal{N}_Q^{(J)}\}$. This fact will reduce (6.1) to a linear problem! Otherwise we could stop and try another subset J of rows of Q.

(6.3) Let $m_1 = ld(\underline{a}_1), ..., m_l = ld(\underline{a}_l)$ be the set of leading monomials of the minimal generating system of $\mathcal{M}(Q) = \langle A\rangle$, formed by the columns of A, cf. (5.2). Take the first index $s \leq l$ such that m_s is not a leading term of $\langle A_0\rangle$. Let $R^k(m_s)$, resp. $R^k_+(m_s)$, denote the quotient of R^k by the submodule of all monomials greater than or equal to m_s, resp. strictly greater than m_s, with respect to the monomial order of R^k.
By our choice, $\langle A_0\rangle$ and $\mathcal{M}(Q)$ have the same image in $R^k(m_s)$ and $\langle A_0\rangle$ is still the unique minimal a an $R^k_+(m_s)$-submodule. It is therefore of K-codimension 1 with respect to $\mathcal{M}(Q)$. Subsequentely, any strict reduction $\mathcal{M}(U_TQ)$ of $\mathcal{M}(Q)$ in $R^k_+(m_s)$ will induce $\langle A_0\rangle$ in $R^k_+(m_s)$.

(6.4) By construction we have $a_j \equiv 0$ for $j > s$ in $R_+(m_s)$; hence, $\mathcal{M}(U_TQ)$ is determined by the submatrix $N_T^{(s)}$ of the first s columns of N_T.

Proposition 12
Let $minor(i) = minor(N_*^{(i)}) \subset K[Z]$ be the ideal of i-minors from the first i rows of N_*. Then

- *(i1) $minor(s-1) = (1)$,*
- *(i2) $minor(s) \neq (1)$.*
- *(i3) If Q splits with respect to J, then the linear space spanned by the columns of $N_*^{(s)}(\underline{z})$: $\langle N_*^{(s)}(\underline{z})\rangle$ is either K^s or a fixed hyperplane $H \subset K^s$ in case $\underline{z}$ is a zero of the ideal $minor(s)$.*

In other words, if $\langle N_*^{(s)}(\underline{z})\rangle$ is dependent of the choice of a zero $\underline{z}$ from $minor(s)$, then Q does not J-split!
$(i1)$ and $(i2)$ hold by our choice of s. If $\underline{z}$ is a zero of $minor(s)$, then for $N_*(\underline{z}) = N_T$

$$\mathcal{M}(U_TQ) \equiv \langle A_0\rangle \quad \text{over} \quad R_+(m_s).$$

(6.5) If Q is J-split, the set of zeros of the ideal $minor(s)$ form a linear subspace with respect to Z:

Proposition 13
If Q is J-split, the radical of $minor(s)$ is generated by linear polynomials.

Note that the radical of an ideal may be computed by just taking annihilators of certain Ext-groups (cf. [EV]). This method is implemented as a procedure in SINGULAR, using only syzygy- and standard-basis-computations. Hence finding a J-row-reduction reduces to solving linear equations if there exists a unique minimal.
Let $N_0 = N^{(s)}(\underline{z})$ and $\underline{z}$ be a zero of $minor(s)$. Then $\operatorname{rk} N_0 = s-1$, and consequently Then regular constant matrices $\Lambda \in Gl_s(K)$, $\tilde{\Lambda} \in Gl_n(K)$ exist such that

$$\Lambda N_0 \tilde{\Lambda} = \begin{pmatrix} I_{s-1} & 0 \\ 0 & 0 \end{pmatrix} =: \tilde{I}_{s-1}.$$

Moreover, $minor(s) = minor(\Lambda N_*^{(s)}\tilde{\Lambda})$. Because $\langle N_*^{(s)}(\underline{z})\rangle$ is independent of the choice of a zero $\underline{z}$ of $minor(s)$, the same holds for $\langle \Lambda N_*^{(s)}\tilde{\Lambda}\rangle$. Therefore, $\underline{z}$ is a zero of $minor(s)$ if and only if $\langle \Lambda N_*^{(s)}(\underline{z})\tilde{\Lambda}\rangle = \langle \Lambda N_0\tilde{\Lambda}\rangle = \langle \tilde{I}_{(s-1)}\rangle$ if and only if the s-th row of $\Lambda N_*^{(s)}(\underline{z})\tilde{\Lambda}$ is identically zero. By construction, all entries of N_*, and so the entries of $\Lambda N_*^{(s)}\tilde{\Lambda}$, are linear polynomials in Z.

(6.6) Note that the minor ideal need not to be reduced, as demonstrated by the following example:
Given $Q = \begin{pmatrix} x & -y \\ y & x-2y \end{pmatrix}$, then a representative in the sense of (5.2) is given by

$$\tilde{Q} = \begin{pmatrix} x & -y & 0 \\ y & x-2y & x^2-2xy+y2 \end{pmatrix}.$$

None of the matrices of $I\!B_+$ increase $\mathcal{M}(Q)$; that is, $\mathcal{N}_Q^{(1)} = \mathrm{Mat}\,(1,1;K[[x,y]])$.
A generator is given by $U_T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $T = (1)$. Then $\tilde{T} = \begin{pmatrix} 0 & 1 & x+y \\ -1 & 2 & x-y \\ 0 & 0 & 0 \end{pmatrix}$, $\tilde{T}_0' = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$ and $\tilde{T}_0'' = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Thus $N_* = \begin{pmatrix} 1 & Z \\ -Z & 1+2Z \end{pmatrix}$, and $minor(N_*) = (1 + 2Z + Z^2) = (1+Z)^2$ is not reduced.

7 Finiteness

To complete the algorithm we have to show the finiteness of the row-reduction process.

Proposition 14
After a finite number of reductions, $\mathcal{M}(Q)$ becomes J-row-minimal.

Assume there is an infinite sequence of row-reductions

$$\mathcal{M}(Q) \supset \mathcal{M}(U_{T_1}Q) \supset \mathcal{M}(U_{T_2}Q)\ldots$$

By our choice of the reduction in Proposition 14, at any step the lowest possible leading term of $\mathcal{M}(Q)$ is removed. But all leading terms of a standard basis of $\mathcal{M}(Q)$ are leading terms of a standard basis of $\langle Q\rangle$, too, which determines the Hilbert-function of the module $M = coker(Q)$. Let r_M be the regularity bound of the Hilbert function of M. Then the homogeneous degree of all leading terms of a standard basis of Q (resp. of $\mathcal{M}(Q)$) is not greater than r_M, contradicting our assumption of an infinite reduction sequence.

8 APPENDIX: The Algorithm

For any strict subset J of $\{1,\ldots,r\}$, $k = card(J)$, we have to apply the following sequence of procedures. Again, we assume for simplicity $J = J_0 = \{1,\ldots,k\}$. If J allows no splitting, we can omit the test for its complement J'.
First prepare the input matrix Q according to (5.2):
$L :=$ **prepare**(Q,k)
INPUT: Q - a representation matrix of the module, k - an integer.
OUTPUT: $L = A,B,C,D$ - a list of matrices presenting the blocks of a good presentation matrix (B is a zero matrix).

```
Q := std_base(Q)
Q := min_base(Q,k)
L := find_blocks(Q,k)
return L
```

The next procedure computes generators of the module of J-row reductions of Q:

$\tilde{L} :=$ **list_of_reductions**(L)
INPUT: $L = A,B,C,D$ - a list of matrices.
OUTPUT: $\tilde{L} = N_1,\ldots,N_q$ - a list of constant matrices corresponding to generators of $\mathcal{N}_Q^J$.

```
Ã := ko_hom(A,cols(C)+cols(D))
C̃ := kontra_hom(concat(C,D),rows(A))
D̃ := syz(concat(Ã,C̃))
D̃ := sub_matrix(D̃[1..cols(Ã),1..cols(D̃)])
```

$i := 1$
WHILE $i <=$`cols(`$\tilde{D}$`)` DO

    $\tilde{T} :=$ `matrix_of_column(`$\tilde{D}[i]$`,cols(`A`),cols(`C`))`
    $N := \tilde{T}$ `modulo` *maxideal*
    IF $(N \neq 0)$ $\tilde{L} := \tilde{L}, N$
    `next` i

END
`return` $\tilde{L}$

Here **ko_hom** computes the matrix of the map defined by inserting the matrix in the first place of the *Hom*-functor and **kontra_hom** does the same with the second argument.
Next we will test J-row-minimality and possibly find a row-reduction of Q:

$Q, bool, break :=$ **find_reduction**$(L, \tilde{L})$
INPUT: $L = A, B, C, D$ - a list of block matrices of Q,
$\tilde{L} = N_1, \ldots, N_q$ - a list of constant matrices
OUTPUT: Q - a presentation matrix,
bool = FALSE if Q was J-row-minimal,
break = FALSE if there is no unique J-row-minimal.

bool := FALSE
break := TRUE
$N_* :=$ `unit_matrix(rows(`N_i`))` $+ \sum Z_i N_i$
$i := 1$
WHILE $i <=$`cols(`$\tilde{T}$`)` DO

    minor := `minor_of_first_rows(`N_*, i`)`
    minor := `std_base(`*minor*`)`
    IF (*minor* $\neq 1$) {*bool* := TRUE; EXIT}
    `next` i

END
IF (*bool*) *minor* := `radical(`*minor*`)`
IF (`is_not_linear(`*minor*`)`) *break* := FALSE
IF (*break*) $z :=$ `find_zero(`*minor*`)`
$N := N_*(z)$
$A, B := A * N$
$Q := \begin{pmatrix} A & B \\ C & D \end{pmatrix}$
`return` Q, *bool*, *break*

In the main loop a J-row-minimal presentation matrix is iterated or we obtain the answer, according to Proposition 13, that there is no J-row-splitting of the module.

$Q, bool :=$ **row_minimize**(Q, k)
INPUT: as above
OUTPUT: Q - a matrix being J-row-minimal if *bool* = TRUE
or Q does not have a unique J-row-minimal presenatation matrix otherwise.

$bool$:= TRUE
$break$:= TRUE
WHILE $bool$ `and` $break$ DO

L `:=` `prepare(`Q,k`)`
$\tilde{L}$ `:=` `list_of_reductions(`L`)`
$Q, bool, break$ `:=` `find_reduction(`$L,\tilde{L}$`)`

END
`return` $Q, break$

If $break$ = TRUE, a final test, which uses Corollary 8, must be preformed to determine whether the presentation matrix allows a J-splitting. Otherwise we shall take the next subset J.

$Q_0, bool :=$ **splitting_test**(Q,k)
INPUT: as above
OUTPUT: Q_0 - a block diagonal presentation matrix if $bool$ = TRUE

L `:=` `prepare(`Q,k`)`
$\tilde{A}$ `:=` `kontra_hom(`A`,rows(`D`))`
$\tilde{D}$ `:=` `ko_hom(`D`,cols(`A`))`
$\tilde{E}$ `:=` `concat(`$\tilde{A},\tilde{D}$`)`
$\tilde{C}$ `:=` `matrix_to_vector(`C`)`
$bool$ `:=` `is_liftable(`$\tilde{E},\tilde{C}$`)`
$Q_0 := \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$
`return` $Q_0, bool$

Remarks:

1. It may happen that the procedure **find_reduction** will not give a result in a reasonable amount of time for J, but for the complement J'. Therefore, it is worth finding good strategies for the algorithm.

2. The procedures and algorithms described here are implemented in the library `module.lib` of the Computer Algebra system SINGULAR [GPS97]. See the accompanying documentation for more details. `module.lib` will be included in a forthcoming new release of SINGULAR and, in the meantime, may be obtained directly from the authors.

References

[HP] J. Herzog, D. Popescu, Thom-Sebastiani problems for maximal Cohen-Macaulay modules. Preprint, Göttingen (1995).

[Yo] Y. Yoshino, *Cohen–Macaulay modules over Cohen–Macaulay rings.* London Math. Soc. Lect. Notes, Ser. 146, Cambridge (1990)

[MPP] B. Martin, G. Pfister, D. Popescu, *Maximal Cohen-Macaulay modules over rings of type* $x^3 + y^t$. Prepr. BTU Cottbus, Mathematik-03/1996

[EV] D. Eisenbud, C. Huneke, W. Vasconcelos, *Direct methods for primary decomposition.* Invent. Math. 110, 207-235 (1992)

[GPS97] G.-M. Greuel, G. Pfister, and Hans Schönemann. Singular Reference Manual. In *Reports On Computer Algebra*, number 12. Centre for Computer Algebra, University of Kaiserslautern, May 1997. `http://www.mathematik.uni-kl.de/~zca/Singular`

List of papers published in the Reports on Computer Algebra series

[1] H. Grassmann, G.-M. Greuel, B. Martin, W. Neumann, G. Pfister, W. Pohl, H. Schönemann, and T. Siebert. Standard bases, syzygies and their implementation in singular. 1996.

[2] H. Schönemann. Algorithms in singular. 1996.

[3] R. Stobbe. FACTORY: a C++ class library for multivariate polynomial arithmetic. 1996.

[4] O. Bachmann and H. Schönemann. A Manual for the MPP Dictionary and MPP Library. 1996.

[5] O. Bachmann, S. Gray, and H. Schönemann. MPP: A Framework for Distributed Polynomial Computations. 1996.

[6] G.M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and syzygies. 1996.

[7] G.M. Greuel. Description of SINGULAR: A computer algebra system for singularity theory, algebraic geometry, and commutative algebra. 1996.

[8] T. Siebert. On strategies and implementations for computations of free resolutions. September 1996.

[9] B. Reinert. Introducing reduction to polycyclic group rings – a comparison of methods. October 1996.

[10] O. Bachmann, S. Gray, and H. Schönemann. A proposal for syntactic data integration for math protocols. January 1997.

[11] O. Bachmann. Effective simplification of cr expressions. January 1997.

[12] O. Bachmann, S. Gray, and H. Schönemann. MP Prototype Specification. January 1997.

[13] O. Bachmann. MPT – a library for parsing and Manipulating MP Trees. January 1997.

[14] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. September 1997.

[15] B. Martin and T. Siebert. Splitting Algorithm for vector bundles. September 1997.

[16] K. Madlener and B. Reinert. String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings. October 1997.

[17] Thomas Siebert. An algorithm for constructing isomorphisms of modules. January 1998.

[18] O. Bachmann and H. Schönemann. Monomial Representations for Gröbner Bases Computations. January 1998.

[19] B. Reinert, K. Madlener, and T. Mora. A note on nielsen reduction and coset enumeration. February 1998.