ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 395–429

JOURNAL OF PURE AND APPLIED ALGEBRA

An algorithm for the Quillen–Suslin theorem for monoid rings

Reinhard C. Laubenbacher [a,*], Cynthia J. Woodburn [b]

[a] *Department of Mathematics, New Mexico State University, Las Cruces, NM 88003, USA*
[b] *Department of Mathematics, Pittsburg State University, Pittsburg, KS 66762-7502, USA*

Abstract

Let k be a field, and let M be a commutative, seminormal, finitely generated monoid, which is torsionfree, cancellative, and has no nontrivial units. Gubeladze [8] proved that finitely generated projective modules over kM are free. This paper contains an algorithm for finding a free basis for a finitely generated projective module over kM. As applications one obtains new algorithms for the Quillen–Suslin Theorem for polynomial rings and Laurent polynomial rings, based on Quillen's proof. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 13C10, 13P10, 14Q15, 19A49

1. Introduction

In 1955, Serre remarked in [15, p. 243] that it was not known whether there exist finitely generated projective modules over $k[x_1,\ldots,x_r]$, k a field, which are not free. This remark turned into the "Serre Conjecture", stating that indeed there were no such modules. Proven in 1976 independently by Quillen [14] and by Suslin [17], it became subsequently known as the Quillen–Suslin Theorem (QS).

In 1978, Anderson [2] conjectured that QS holds for affine normal subrings of polynomial rings generated by monomials, that is, that all finitely generated projective modules over such rings are free. In 1988, Gubeladze [8] proved this conjecture, and showed that QS holds exactly for monoid rings of seminormal monoids. For normal monoids, this says in geometric language that algebraic vector bundles over affine toric varieties are trivial (see [6, p. 31]).

* Corresponding author. E-mail: reinhard@nmsu.edu.

PII S0022-4049(97)00020-0

Several algorithms have been given for QS over polynomial rings [4, 5, 11]. Given a finitely generated projective module over $k[x_1,\ldots,x_r]$, k a field, presented as the cokernel of a matrix with polynomial entries, these algorithms produce a free basis for the module. See [20] for applications of these algorithms to problems in control theory. From the point of view of solving linear systems of equations with polynomial coefficients, one may interpret the theorem as follows. Let A be an $n \times m$-matrix with entries in $R = k[x_1,\ldots,x_r]$, and let

$$A \cdot y = 0$$

be a system of linear equations. Define a module P via the presentation

$$R^m \xrightarrow{A} R^n \longrightarrow P \longrightarrow 0,$$

and suppose that P is a projective R-module. Then the Quillen–Suslin theorem implies that the solution space of the system $Ay = 0$ has a free basis, and an algorithm for the theorem will compute such a free basis.

This paper contains an algorithm for QS over seminormal monoid rings, which we will call the *QS-algorithm*. One way to interpret this algorithm in a special case is that if the matrix A above has entries which are "sparse" polynomials, in the sense that the exponent vectors of appearing monomials lie in a pre-specified submonoid of $\mathbf{N}^r$, and suppose that $n \leq m$, and the $(n \times n)$-minors of A span the unit ideal, then the QS-algorithm produces $m - n$ polynomial vectors with the same "monomial sparsity pattern" which freely span the cokernel of A.

As an example, suppose that $R = k[x, y]$, and that the matrix A contains only monomials from the subring $k[xy, x^2y, xy^2] \subset k[x, y]$, i.e., the exponent vectors of all monomials appearing in A lie in the submonoid M of $\mathbf{N}^2$ generated by the three vectors $(1,1),(1,2),(2,1)$. Observe that

$$k[xy, x^2y, xy^2] \cong k[u,v,w]/(vw - u^3) \cong kM,$$

where kM is the monoid ring of M. Thus, finding an algorithm for QS over the subring $k[xy, x^2y, xy^2]$ is equivalent to finding such an algorithm over the monoid ring kM. If we choose A to be the matrix $(xy, xy^2 - 1, x^2y + xy + 1)^t$, then A is defined over our subring. There is an obvious way to reduce A to the matrix $(1,0,0)$, but that involves polynomials not in the subring.

As a corollary we obtain a QS-algorithm for Laurent polynomial rings (Corollary 42). Such an algorithm was first given by Park [12]. We also obtain an alternative version of the QS-algorithm for polynomial rings (Corollary 23). It differs from the existing algorithms in that it relies on Quillen's proof rather than on Suslin's. All essential ingredients of the algorithm are implicitly (and, in some cases, explicitly) contained in [8] and Swan's exposition [19] of Gubeladze's result. All rings which appear are either subrings of polynomial rings over a field, or quotients of polynomial rings, or localizations thereof. Thus, all required computations can be carried out using the theory of Gröbner bases, as described in [1, 3, 10]. Finally, since the study of projective

modules is properly part of algebraic K-theory, the present paper may be considered a contribution to the computational side of that subject.

We now give a precise statement of the result.

Theorem 1. *Let k be a field, and let M be a finitely generated, commutative, torsion free, seminormal, cancellative monoid without nontrivial units. If P is a finitely generated projective module over the monoid ring kM, given as the cokernel of a matrix with entries in kM, then there is an algorithm to compute a free basis for P.*

We will call such monoids *toric*, since, if M is normal, then the monoid ring kM is isomorphic to the coordinate ring of an affine toric variety, and conversely. The contents of the paper are as follows. Section 2 contains a summary of definitions and results from [8, 19] pertaining to toric monoids that will be needed subsequently. In Section 3 we describe algorithms to carry out "Milnor patching" for certain kinds of pullback squares. That is, given a commutative square of rings

$$\begin{array}{ccc} R & \longrightarrow & R_1 \\ \downarrow & & \downarrow \\ R_2 & \longrightarrow & \bar{R} \end{array}$$

such that

$$R \cong \{(r_1, r_2) \in R_1 \times R_2 \mid \bar{r}_1 = \bar{r}_2 \text{ in } \bar{R}\},$$

then, with certain extra hypotheses, projective modules over R can be obtained by "patching together" pairs of projective modules over R_1 and R_2.

In Section 4, we reduce the problem for normal toric monoids M to finding an algorithm for the "interior" submonoid M^* of M. In Section 7, we construct a certain sequence of submonoids of M

$$M = M_0, M_1, \ldots, M_k = F,$$

ending in a free monoid F. In Sections 5 and 6 we construct algorithms to show that this sequence has the property that projective modules over kM_i are obtained from projective modules over kM_{i+1} by restriction or extension of scalars. Since kF is just a polynomial ring, we can use one of the existing algorithms for the "ordinary" QS.

In Section 8, we summarize the different steps of the algorithm in their natural order. As an application we give an algorithm for QS for Laurent polynomial rings, first proven by Swan [18].

The QS-algorithm proceeds by induction on the rank of the monoid M. If $\mathrm{rk}(M) = 1$, then kM is simply a polynomial ring in one variable over k, so the desired algorithm is just the Smith normal form. Thus, we will from now on assume the following:

Induction Hypothesis 1. *There is a QS-algorithm for all fields and all toric monoids of rank less than the rank of M.*

2. Toric monoids

All monoids in this paper are assumed to be commutative. We write $\langle g_1,\ldots,g_t\rangle$ to denote the monoid generated by the elements $g_1,\ldots,g_t$. Generally, we will write monoids multiplicatively, except in the examples, which are all given as submonoids of $\mathbf{N}^d$ for some d.

Definition 2. A monoid is said to be *torsion free* if $x = y$ whenever $x^n = y^n$ for some integer $n > 0$. It is *cancellative* if $ax = ay$ implies $x = y$.

Note that the condition that M be torsion free and cancellative is equivalent to the monoid ring kM being a domain.

For each cancellative torsion free monoid M, there exists an abelian group $\mathrm{gp}(M)$ which contains M (or at least an isomorphic copy of M), and which is the smallest such group, called the group completion of M. Furthermore, $\mathrm{gp}(M)$ is unique up to isomorphism. The *rank* of M, denoted $\mathrm{rk}(M)$, is defined to be the rank of $\mathrm{gp}(M)$.

Definition 3. A monoid M is *seminormal* if $x \in \mathrm{gp}(M)$ and $x^2, x^3 \in M$ implies $x \in M$, and *normal* if $x \in \mathrm{gp}(M)$ and $x^n \in M$ for some $n > 0$ implies $x \in M$. The *normalization* of a torsion free monoid M in a group G is

$$\widetilde{M} = \{x \in G \mid x^n \in M \text{ for some } n > 0\}.$$

Example 4. An example of a monoid which is seminormal but not normal is

$$M = \langle (2,3),(3,5),(3,6),(1,1),(2,1)\rangle \subset \mathbf{N}^2.$$

The normalization of M is $\widetilde{M} = \langle (1,2),(1,1),(2,1)\rangle$.

Definition 5. We will call a monoid M *toric* if M is finitely generated, torsion free, cancellative, seminormal, and has no nontrivial units.

Since a toric monoid M can be naturally embedded in the real vector space $\mathbf{R} \otimes_{\mathbf{Z}} \mathrm{gp}(M)$ [19, p. 224], we can view M as a subset of $\mathbf{N}^d$. So a normal toric monoid M can be defined as

$$M = \{(a_1,\ldots,a_d) \in \mathbf{N}^d \mid (a_1,\ldots,a_d)\cdot A \leq 0\},$$

for some matrix A with d rows, where each row of A corresponds to a bounding hyperplane of M in $\mathbf{R}^d$ [6, p. 9]. (M must be normal in this situation, since we are defining it as the set of *all* lattice points satisfying a collection of linear inequalities.) For example,

$$\begin{aligned} M &= \langle (1,2),(1,1),(2,1)\rangle \\ &= \left\{(a_1,a_2) \in \mathbf{N}^2 \mid (a_1,a_2)\begin{pmatrix} -2 & 1 \\ 1 & -2 \end{pmatrix} \leq (0,0)\right\} \end{aligned}$$

has bounding hyperplanes $-2x+y=0$ and $x-2y=0$ in $\mathbf{R}^2$. Whenever M is given in this manner, that is, as the solution set of a system of linear inequalities, it is an integer programming problem to find a minimal generating set for M. Such a generating set, called a Hilbert basis, can be found by means of an algorithm such as the one given in [16, pp. 22–23], which uses Gröbner basis theory.

Definition 6. The *interior* of a monoid M is

$$\mathrm{Int}(M) = \{x \in M \mid \text{for each } y \in M \text{ there are } n > 0, z \in M \text{ with } x^n = yz\}.$$

We use the notation M^* to denote the submonoid $\mathrm{Int}(M) \cup \{1\}$.

Observe that M^* need not be finitely generated, even if M is. If the rank of M is finite, then M and M^* will have the same rank, however.

Definition 7. A nonempty submonoid E of a monoid M is *extremal* whenever $x, y \in M$ with $xy \in E$ implies $x, y \in E$.

Notice that if we consider $M \subset \mathbf{N}^d$, it is not difficult to verify that extremal submonoids of a toric monoid M lie on bounding hyperplanes of M [19, Theorem 5.4].

Lemma 8. *If $M = \langle g_1, \ldots, g_t \rangle$ is a toric monoid with $\mathrm{gp}(M) = \mathbf{Z}^d$, then generators for all extremal submonoids of M can be found.*

Proof. We will write M additively. First, we eliminate from consideration those generators of M which lie in $\mathrm{Int}(M)$. Since $g \in \mathrm{Int}(M)$ if and only if $M[-g] = \{\sum_{j=1}^{t} a_j g_j - bg \mid a_j, b \in \mathbf{N}\} = \mathrm{gp}(M) = \mathbf{Z}^d$ [19, Lemma 9.5], testing whether $g \in \mathrm{Int}(M)$ amounts to solving a system of $2d$ linear equations over $\mathbf{N}$. Once each generator of M has been tested for membership in $\mathrm{Int}(M)$, let $S = \{s_1, \ldots, s_q\}$ be the largest subset of generators of M contained in the complement of $\mathrm{Int}(M)$.

Next, using the set S, we begin forming maximal extremal submonoids of M, relying on the fact that if E is an extremal submonoid of M then $E \cap S$ is a generating set for E [19, p. 225]. Starting with s_1, consider $\langle s_1, s_2 \rangle$. We need to know whether or not $\langle s_1, s_2 \rangle \cap \mathrm{Int}(M) = \emptyset$. Note that $\langle s_1, s_2 \rangle \cap \mathrm{Int}(M) \neq \emptyset$ if and only if $\mathbf{Z}^d = \left\{\sum_{j=1}^{t} a_j g_j - b_1 s_1 - b_2 s_2 \mid a_j, b_i \in \mathbf{N}\right\}$, so again this involves solving systems of linear equations over $\mathbf{N}$. If $\langle s_1, s_2 \rangle \cap \mathrm{Int}(M) = \emptyset$, then $\langle s_1, s_2 \rangle$ is contained in some extremal submonoid of M [19, Lemma 5.1]. We can find a maximal such extremal monoid by continuing this process to enlarge the set of generators as much as possible. If $\langle s_1, s_2 \rangle \cap \mathrm{Int}(M) \neq \emptyset$, then consider $\langle s_1, s_3 \rangle$. Repeating the process by considering all possible combinations of elements of S, we can obtain all maximal extremal submonoids of M. If we repeat the process on each submonoid so obtained and continue in this manner until the process terminates, we will have obtained the set of all extremal submonoids of M. □

An algorithm to find the extremal submonoids of M is implemented in the program PORTA (see [21, Lecture 0]).

Lemma 9. *Let M be a toric monoid. Then generators for the normalization of M can be found.*

Proof. By [19, Lemma 6.6], M and its normalization $\widetilde{M}$ have the same interior, i.e., $\mathrm{Int}(M) = \mathrm{Int}(\widetilde{M})$. Let E be an extremal submonoid of M. Notice that M being seminormal implies E is also seminormal. For if $x^2, x^3 \in E$ for some $x \in \mathrm{gp}(E)$, then $x \in M$. Consequently, by the definition of extremal submonoid, $x \in E$. Thus, an extremal submonoid of $\widetilde{M}$ is the normalization of an extremal submonoid of M. It is therefore sufficient to find generators for the normalizations of all proper extremal submonoids of M, which can be accomplished by computing Hilbert bases of the bounding hyperplanes of M, since each proper extremal submonoid of M lies on a bounding hyperplane of M [19, Theorem 5.4]. □

The algorithm for the following result was suggested by one of the referees.

Lemma 10 (Swan [19, Lemma 11.2]). *Given a toric monoid $M = \langle g_1, \ldots, g_t \rangle$, there exists a free monoid F contained inside M^* with $\mathrm{gp}(F) = \mathrm{gp}(M)$.*

Proof. Since $\mathrm{gp}(M)$ is a free abelian group, we may assume that it is equal to $\mathbf{Z}^d$ for some $d \geq 1$. Choose an element $z \in \mathrm{Int}(M)$, for instance, let $z = g_1 + \cdots + g_t$. Using the Euclidean algorithm, z can be extended to a basis $z = z_1, \ldots, z_d$ of $\mathbf{Z}^d$. (Note that this amounts to carrying out a QS-algorithm for $\mathbf{Z}$). Now choose N large enough such that $z_i + Nz_1 \in M^*$ for all $i = 1, \ldots, d$. Then $z_1, z_2 + Nz_1, \ldots, z_d + Nz_1$ is a free basis for a free monoid F contained in M^* such that $\mathrm{gp}(F) = \mathrm{gp}(M) = \mathbf{Z}^d$. □

Lemma 11. *Given two normal toric submonoids N_1 and N_2 of a toric monoid M, then one can compute generators for the normal toric submonoid $N_1 \cap N_2$ of M.*

Proof. Let $N_1 = \{(a_1, \ldots, a_d) \in \mathbf{N}^d \mid (a_1, \ldots, a_d) \cdot A_1 \leq 0\}$, and $N_2 = \{(a_1, \ldots, a_d) \in \mathbf{N}^d \mid (a_1, \ldots, a_d) \cdot A_2 \leq 0\}$, where A_1 and A_2 are the coefficient matrices of the systems of linear inequalities corresponding to the bounding hyperplanes of N_1 and N_2, respectively. Then $N_1 \cap N_2 = \{(a_1, \ldots, a_d) \in \mathbf{N}^d \mid (a_1, \ldots, a_d) \cdot B \leq 0\}$, where $B = (A_1 | A_2)$. Consequently, generators for $N_1 \cap N_2$ can be found by computing a Hilbert basis for the system of linear inequalities formed by considering the bounding hyperplanes of both submonoids. □

Definition 12. Let M be a normal toric monoid and let $\psi : M \to \mathbf{N}$ be a homomorphism with $\psi^{-1}(0) = \{1\}$. (For example, ψ might be the defining equation for a hyperplane H such that $H \cap M = \{1\}$.) Let m be a positive integer and $z \in \mathrm{Int}(M)$.

Then the *homothetic transformation* θ_m with center z is the map

$$\begin{aligned}\theta_m : M &\to M\\ x &\mapsto x^m z^{\psi(x)}.\end{aligned}$$

A *homothetic submonoid* $M^{(m)}$ of M with center z is the normalization of the image $\theta_m(M)$ in $\mathrm{gp}(M)$. (Note that $M^{(m)} \subset M^*$.)

Lemma 13. *Let $M = \langle g_1, \ldots, g_t \rangle$ be a normal toric monoid and $z \in \mathrm{Int}(M)$. Then a finite generating set for the mth homothetic submonoid $M^{(m)}$ of M can be found.*

Proof. By Lemma 8, we can find generators for each of the maximal extremal submonoids $\{E_1, \ldots, E_p\}$ of M. Note that the generators of each E_i lie on some bounding hyperplane of M [19, Theorem 5.4]. Therefore, the images of the generators of E_i under the homothetic transformation will lie on a bounding hyperplane of $M^{(m)}$. Thus, $M^{(m)}$ is the solution set to the system of linear inequalities resulting from applying the homothetic transformation to each E_i, and computing a Hilbert basis for the system will yield a generating set for $M^{(m)}$. □

Lemma 14 (Swan [19, Lemma 9.6]). *Let $M = \langle g_1, \ldots, g_t \rangle$ be a normal toric monoid and N a finitely generated submonoid such that $\mathrm{gp}(N) = \mathrm{gp}(M)$. Let $\theta_m : M \to M$ be a homothetic transformation with center z for some $z \in \mathrm{Int}(N)$ and $m \in \mathbf{N}$. Then one can find $s \in \mathbf{N}$ such that $(\theta_m)^s(M) \subset N^*$.*

Proof. Since $\langle z^{-1}, N \rangle = \mathrm{gp}(N) = \mathrm{gp}(M)$ [19, Lemma 9.5], by repeatedly multiplying by z, we can find a p such that $z^p g_i \in \mathrm{Int}(N)$ for all i. Let $s = pm$. Then $(\theta_m)^s(g_i) \in \mathrm{Int}(N) \subset N^*$ for each i, and hence $(\theta_m)^s(M) \subset N^*$, as desired. □

Lemma 15. *Let M be a toric monoid, N a submonoid of the same rank as M. Let $x \in \mathrm{Int}(N)$, $y \in M$. Then there exists an integer $n \geq 0$ such that $x^n y \in \mathrm{Int}(N)$.*

Proof. Since N and M have the same rank, we have $\mathrm{gp}(N) = \mathrm{gp}(M)$. Recall that $x \in \mathrm{Int}(N)$ if and only if $N[x^{-1}] = \mathrm{gp}(N)$. Therefore we can find $z \in N$ and $n' \geq 0$ such that $y = x^{-n'} z$. Hence $x^{n'} y = z \in N$, and consequently $x^{n'+1} y = x^n y \in \mathrm{Int}(N)$. □

3. Milnor patching

In this section we derive an algorithmic version of a process for constructing projective modules using pullback squares, commonly referred to as "Milnor patching," for some special types of so-called Milnor squares and Karoubi squares. First we consider Milnor squares.

Let R_1, R_2 be commutative rings with a common quotient ring $\bar{R}$. Assume furthermore that the quotient map $f : R_1 \longrightarrow \bar{R}$ is a split surjection. Now consider the pullback square

$$\begin{array}{ccc} R & \longrightarrow & R_1 \\ \downarrow & & \downarrow f \\ R_2 & \longrightarrow & \bar{R}, \end{array}$$

where $R = \{(r_1, r_2) \in R_1 \times R_2 \mid \bar{r}_1 = \bar{r}_2\}$. Such a square is a special case of a *Milnor square*. (For a discussion of more general Milnor squares see [19, Section 2].)

Algorithm 1 (Patching)

Input: A finitely generated projective R_1-module P, of rank r, given as the cokernel of a matrix

$$R_1^n \xrightarrow{A} R_1^m \longrightarrow P \longrightarrow 0.$$

Suppose we are also given an isomorphism

$$\alpha : \bar{P} \longrightarrow \bar{R}^r.$$

That is, we have a commutative diagram:

$$\begin{array}{ccccccc} \bar{R}^n & \xrightarrow{\bar{A}} & \bar{R}^m & \longrightarrow & \bar{P} & \longrightarrow & 0 \\ = \downarrow & & \downarrow \bar{B} & & \cong \downarrow & & \\ \bar{R}^n & \xrightarrow{\bar{B}\bar{A}} & \bar{R}^m & \longrightarrow & \bar{R}^r & \longrightarrow & 0 \end{array}$$

with $\bar{B}$ an invertible matrix over $\bar{R}$, such that

$$\bar{B}\bar{A} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}, \tag{1}$$

where the upper left-hand block I is an identity matrix.

Output: A matrix with entries in R, presenting a projective R-module Q, and an R_1-isomorphism from Q to P over R_1, given in the form of a base change matrix for the presentation of P.

Algorithm. As a set,

$$Q = \{(x_1, x_2) \in P \times R_2^r \mid \alpha(\bar{x}_1) = \bar{x}_2\}.$$

We need to compute generators for Q. Since the right-hand vertical map f is a split epimorphism we can lift $\bar{B}$ to an invertible $m \times m$-matrix B over R_1. Then the cokernel of BA is a projective R_1-module P' isomorphic to P via the base change matrix B. Now let Q be the cokernel of the $n \times m$-matrix with entries in R, whose R_1-part is BA and whose R_2-part is (1). Note that this gives indeed a well-defined matrix

over R. Furthermore, upon extending scalars to R_1, respectively R_2, Q extends to P', respectively R_2^r. □

Now we consider a certain type of Karoubi square. Suppose that M is a normal toric monoid, and $N \subset M$ is a nondegenerate pyramidal extension (see Section 6). That is, we have a homomorphism $\delta : M \longrightarrow \mathbf{Z}$, with $N = \{x \in M \mid \delta(x) \leq 0\}$. Furthermore, there exists an element $v \in M$ such that $\delta(v) > 0$, and M is integral over $\langle N, v\rangle$, i.e. for each $x \in M$ there exists $n > 0$ such that $x^n \in \langle N, v\rangle$. Let $\mathscr{M}^*$ be the maximal ideal of kN^* generated by the set $N^* \setminus \{1\}$. Localizing at $\mathscr{M}^*$, we obtain a special case of a *Karoubi square*:

$$\begin{array}{ccc} kN^* & \longrightarrow & kM^* \\ \downarrow & & \downarrow \\ kN^*_{\mathscr{M}^*} & \longrightarrow & kM^*_{\mathscr{M}^*}. \end{array}$$

Algorithm 2 (Patching)

Input: A finitely generated projective kM^*-module P, presented by a matrix A with coefficients in kM^*, and an isomorphism

$$\alpha : P_{\mathscr{M}^*} \xrightarrow{\cong} (kM^*_{\mathscr{M}^*})^t,$$

represented as in the input for the Patching Algorithm 1.

Output: A finitely generated projective kN^*-module Q and an isomorphism from Q to P over kM^*, as in the previous algorithm.

Algorithm. Since kM^* is a domain, there is a short exact sequence of kM^*-modules

$$0 \longrightarrow P \longrightarrow P_{\mathscr{M}^*} \cong (kM^*_{\mathscr{M}^*})^t \longrightarrow L \longrightarrow 0,$$

where the first map is the inclusion and L is the quotient. Restriction of the quotient map gives an exact sequence of kN^*-modules

$$0 \longrightarrow Q \longrightarrow (kN^*_{\mathscr{M}^*})^t \longrightarrow L.$$

It is shown in [8, Lemma 14] that the module Q is a finitely generated projective kN^*-module which extends to P. We now compute a set of generators of Q over kN^* and an explicit isomorphism from Q to P over kM^*.

Let A be an $m \times n$-matrix with entries in kM^* whose cokernel is P. Let U be an invertible $m \times m$-matrix with entries in $kM^*_{\mathscr{M}^*}$ such that

$$U \cdot A = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix},$$

which exists by hypothesis. Thus, we have an exact sequence

$$0 \longrightarrow P \xrightarrow{\text{incl}} P_{\mathscr{M}^*} \xrightarrow{U} (kM^*_{\mathscr{M}^*})^t \longrightarrow L \longrightarrow 0. \tag{2}$$

Let f be a common denominator of the entries in U. Then P becomes free over kM_f^*. We obtain a short exact sequence

$$0 \longrightarrow P \xrightarrow{\text{incl}} P_f \xrightarrow{U} (kM_f^*)^t \longrightarrow L' \longrightarrow 0,$$

which becomes sequence (2) upon extension of scalars to $kM^*_{M^*}$. The kernel K of the projection $(kM_f^*)^t \longrightarrow L'$ is generated as a kM^*-module by the projection of the columns of U onto the last t coordinates. Define $Q' = K \cap (kN_f)^t$. In order to compute generators for Q' as a kN^*-module, observe that the elements of K all have denominator f. Thus, Q' is the intersection of K with the kN^*-submodule of $(kN_f^*)^t$ generated by the elements $(1/f, 0, \ldots, 0), \ldots, (0, \ldots, 1/f)$. Then

$$Q = Q' \cap \langle \operatorname{Int} N \rangle_f,$$

where $\langle \operatorname{Int}(N) \rangle$ is the ideal of kN generated by the set $\operatorname{Int}(N)$. The intersections can be computed using Gröbner basis theory, since they involve only submodules of free modules. From the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \longrightarrow & (kN_f^*)^t & \longrightarrow & L' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \text{incl}} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & P & \longrightarrow & (kM_f^*)^t & \longrightarrow & L' & \longrightarrow & 0 \end{array}$$

we obtain an explicit kN^*-monomorphism from Q to P, which becomes an isomorphism upon extending scalars to kM^*. □

4. Reduction to M^*

In this section, let M be a normal toric monoid. We assume the Induction Hypothesis 1, that we can carry out the QS-algorithm for all fields and all toric monoids of rank less than the rank of M.

We now use Milnor patching on a sequence of Milnor squares to reduce the problem to that for monoids of the form M^*. Roughly speaking, we obtain M^* from M by successively deleting extremal submonoids from M, first all those of rank one, then the interiors of those of rank two, etc. Each such deletion is accomplished via a Milnor square in which the right-hand vertical map is a split surjection, so that we can use the Milnor patching algorithm from the previous section.

Lemma 16. *Let $E \subset M$ be an extremal submonoid. Then the ideal I of kM generated by $M \setminus E$ is a prime ideal, and the canonical projection $kM \longrightarrow kM/I$ is a split epimorphism.*

Proof. That I is a prime ideal follows directly from the definition of an extremal submonoid.

Note that there is a canonical isomorphism $kM/I \cong kE$, so the inclusion $kE \longrightarrow kM$ provides a splitting for the projection. □

Algorithm 3 (Reduction to the Interior)

Input: A normal toric monoid M and a finitely generated projective kM-module P.

Output: A finitely generated projective kM^*-module Q and an isomorphism from Q to P over kM.

The algorithm proceeds by induction on the rank of M. As before, if $\mathrm{rk}(M) = 1$, then $M = M^*$, and there is nothing to be done. So assume that $\mathrm{rk}(M) > 1$.

Step 1: Compute all extremal submonoids of M (Lemma 8), and list them in order of increasing rank:

$$M_{01} = \{1\}, M_{11}, M_{12}, \ldots, M_{1n_1}, M_{21}, \ldots, M_{d1} = M,$$

such that M_{ij} has rank i, and the rank of M is d.

Step 2: Construct a sequence of Milnor squares as follows. Let I_{11} be the ideal of kM generated by the set $M \backslash M_{11}$, and let K_{11} be the submonoid $(M \backslash M_{11}) \cup \{1\}$ of M. Then I_{11} is a prime ideal, and we obtain the Milnor square

$$\begin{array}{ccc} kK_{11} & \longrightarrow & kM \\ \downarrow & & \downarrow \\ k & \longrightarrow & kM/I_{11}. \end{array}$$

Note that $kM/I_{11} \cong kM_{11}$, and that therefore the right-hand vertical map is a split surjection. Furthermore, $\mathrm{rk}(M_{11}) < \mathrm{rk}(M)$, so that the Induction Hypothesis 1 applies to M_{11}. Use it to find an isomorphism from the image $\bar{P}$ of P to a free kM/I_{11}-module. Now use the Patching Algorithm 1 to construct a projective kK_{11}-module P_{11}, and an isomorphism to P over kM.

Now consider M_{12}. Since $\mathrm{rk}(M_{11}) = \mathrm{rk}(M_{12}) = 1$, it follows that $M_{11} \cap M_{12} = \{1\}$. Let I_{12} be the ideal of kK_{11} generated by the set

$$K_{11} \backslash (K_{11} \cap M_{12}) = K_{11} \backslash M_{12} = M \backslash (M_{11} \cup M_{12}).$$

Then I_{12} is a prime ideal of kK_{11}, and the canonical surjection

$$kK_{11} \longrightarrow kK_{11}/I_{12} \cong kM_{12}$$

is split by the inclusion $kM_{12} \longrightarrow kK_{11}$. Let K_{12} be the submonoid $K_{11} \backslash (K_{11} \cap M_{12}) \cup \{1\}$. Then we obtain the Milnor square

$$\begin{array}{ccc} kK_{12} & \longrightarrow & kK_{11} \\ \downarrow & & \downarrow \\ k & \longrightarrow & kM_{12} \end{array}$$

with split surjective right-hand map. Now apply the same construction as above to P_{11} in order to obtain a projective kK_{12}-module P_{12}, and an isomorphism to P_{11} over kK_{11}.

Continue in this way through all rank 1 extremal submonoids. The last such Milnor square is of the form

$$\begin{array}{ccc} kK_{1n_1} & \longrightarrow & kK_{1,n_1-1} \\ \downarrow & & \downarrow \\ k & \longrightarrow & kM_{1n_1}. \end{array}$$

Observe that

$$K_{1n_1} = (M \setminus (M_{11} \cup \cdots \cup M_{1n_1})) \cup \{1\}.$$

Now consider the first rank 2 extremal submonoid M_{21}. First observe that $M_{21} \cap K_{1n_1} = M_{21}^*$. Let

$$K_{21} = (K_{1n_1} \setminus M_{21}^*) \cup \{1\}.$$

Furthermore, let I_{21} be the ideal of kK_{1n_1} generated by $K_{1n_1} \setminus M_{21}^*$. Then we obtain the Milnor square

$$\begin{array}{ccc} kK_{21} & \longrightarrow & kK_{1n_1} \\ \downarrow & & \downarrow \\ k & \longrightarrow & kM_{21}^* \end{array}$$

with the right-hand map a split surjection. Since $\mathrm{rk}(M_{21}) < \mathrm{rk}(M)$, we may assume by induction that there is a QS-algorithm for kM_{21}^*.

Continuing in this fashion we finally arrive at the Milnor square

$$\begin{array}{ccc} kM^* & \longrightarrow & kK_{d-1,n_{d-1}-1} \\ \downarrow & & \downarrow \\ k & \longrightarrow & kM_{d-1,n_{d-1}}. \end{array}$$

We have constructed a projective kM^*-module $Q = P_{d-1,n_d-1}$ and an isomorphism to P over kM. □

5. The induction step

This section contains the key result needed for the induction step of the QS-algorithm. Several subalgorithms are needed. The first one concerns a special case of the Quillen patching theorem [19, Theorem 3.1]. The algorithm for its proof is a variant of the algorithm in [11], incorporating part of the algorithm in [13].

Proposition 17. *Let M be a normal toric monoid, and let $R = kM[x]$ be the polynomial ring in one variable over kM. Let P be a finitely generated projective R-module. Suppose that one can compute a free basis for $P_{\mathcal{M}}$ for all maximal ideals $\mathcal{M}$*

of kM, and furthermore that there is a QS-algorithm for kM. Then P is free, and there is an algorithm to find a free basis for P.

Proof and algorithm. Represent kM as $k[x_1,\ldots,x_t]/I$ where I is the binomial ideal generated by the defining relations of M [7, Theorem 7.1]. Then

$$R = kM[x] = k[x_1,\ldots,x_t,x]/I.$$

Suppose that P has rank r, and a free presentation:

$$R^n \xrightarrow{A} R^m \longrightarrow P \longrightarrow 0,$$

where A is an $(m \times n)$-matrix with entries in R and rank $m-r$. Then P is free if and only if there exists an invertible $m \times m$-matrix U over R and a commutative diagram

$$\begin{array}{ccccccc} R^n & \xrightarrow{A} & R^m & \longrightarrow & P & \longrightarrow & 0 \\ \| & & \downarrow U & & \downarrow \cong & & \\ R^n & \xrightarrow{B} & R^m & \longrightarrow & R^r & \longrightarrow & 0, \end{array}$$

such that

$$B = U \cdot A = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix},$$

where I is an identity matrix of size $(m-r)\times(m-r)$. We now construct a sequence of maximal ideals of kM as follows. Let $a_1 \in \bar{k}^t$ be a common root for the generators of I in an algebraic closure $\bar{k}$ of k, and let

$$\widetilde{\mathcal{M}_1} = \{f \in k[x_1,\ldots,x_t] \mid f(a_1) = 0\}.$$

Then $\widetilde{\mathcal{M}_1}$ is a maximal ideal of $k[x_1,\ldots,x_t]$ which contains I. Thus, it corresponds to a maximal ideal $\mathcal{M}_1$ of kM.

We will subsequently write $A(x)$, etc., to indicate that a given matrix is defined over the ring $kM[x]$, so that $A(0)$ becomes a matrix over kM. Let $U_1(x) \in \mathrm{GL}_m(kM_{\mathcal{M}_1}[x])$ be such that

$$U_1(x) \cdot A(x) = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix};$$

such a U_1 can be computed by hypothesis. Let $r_1 \in kM$ be a common denominator for all the entries in U_1. Then $r_1 \notin \mathcal{M}_1$, by construction. Lift r_1 to $\tilde{r}_1 \in k[x_1,\ldots,x_t]$, and let a_2 be a common zero of the elements in I and $\tilde{r}_1$. Then define

$$\widetilde{\mathcal{M}_2} = \{f \in k[x_1,\ldots,x_t] \mid f(a_2) = 0\}.$$

As before, $\widetilde{\mathcal{M}_2}$ is a maximal ideal which contains I. Furthermore, it is different from $\widetilde{\mathcal{M}_1}$, since $\tilde{r}_1 \in \widetilde{\mathcal{M}_2} \setminus \widetilde{\mathcal{M}_1}$. So $\widetilde{\mathcal{M}_2}$ corresponds to a maximal ideal $\mathcal{M}_2$ of kM which

contains r_1. Let $U_2(x) \in \mathrm{GL}_m(kM_{\mathscr{M}_2})$ be such that

$$U_2(x) \cdot A(x) = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Define r_2 to be a common denominator for all entries in U_2, with lifting $\tilde{r}_2 \in k[x_1, \ldots, x_t]$. Note that $r_2 \notin \langle r_1 \rangle$, since $r_1 \in \mathscr{M}_2$ but $r_2 \notin \mathscr{M}_2$.

Continuing this construction, we obtain $r_3 \notin \langle r_1, r_2 \rangle$, and so on. Since kM is noetherian, we must reach a point where

$$\langle r_1, \ldots, r_s \rangle = kM.$$

Then, for every $d \geq 1$, we can find $g_1, \ldots, g_s \in kM$ such that

$$r_1^d g_1 + \cdots + r_s^d g_s = 1.$$

This holds in particular for $d = m$. Introduce new variables u and z and define

$$\Delta_i(u,z) = U_i^{-1}(u+z)U_i(u)$$

for $i = 1, \ldots, k$. Then $\Delta_i(u,z)$ is invertible, with entries in $kM_{\mathscr{M}_i}[u,z]$. Recall that r_i is a common denominator for $U_i(u)$ and $U_i(u+z)$. Since

$$U_i^{-1}(u+z) = \det(U_i(u+z)) \cdot \mathrm{adj}(U_i(u+z)),$$

we see that r_i^{m-1} is a common denominator for $U_i^{-1}(u+z)$. Therefore, r_i^m is a common denominator for $\Delta_i(u,z)$. Expand $\Delta_i(u,z)$ as a polynomial in z with matrix coefficients over $kM_{\mathscr{M}_i}[u]$:

$$\Delta_i(u,z) = \Delta_{i0}(u) + \Delta_{i1}(u)z + \cdots + \Delta_{id_i}(u)z^{d_i}.$$

Then $\Delta_{i0}(u) = \Delta_i(u,0) = I_m$. Now replace z by zr_i^m:

$$\Delta_i(u, zr_i^m) = I_m + r_i^m \Delta_{i1}(u)z + r_i^{2m}\Delta_{i2}(u)z^2 + \cdots + r_i^{d_i m}\Delta_{id_i}(u)z^{d_i}.$$

Since r_i^m is a common denominator for $\Delta_i(u,z)$, it is also a common denominator for all $\Delta_{ij}(u)$, so that the above expansion is denominator-free, and $\Delta_i(u, zr_i^m)$ is an invertible matrix over $kM[u,z]$. Observe furthermore that

$$\begin{aligned}
\Delta_i(u, zr_i^m) \cdot A(u) &= U_i^{-1}(u + zr_i^m)U_i(u)A(u) \\
&= U_i^{-1}(u + zr_i^m)\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \\
&= U_i^{-1}(u + zr_i^m)U_i(u + zr_i^m)A(u + zr_i^m) \\
&= A(u + zr_i^m)
\end{aligned}$$

in $kM[u,z]$. Now define

$$\begin{aligned}
U(x) = \Delta_s\left(x - \sum_{i=1}^{s-1} x g_i r_i^m, -x g_s r_s^m\right) \cdot \Delta_{s-1}\left(x - \sum_{i=1}^{s-2} x g_i r_i^m, -x g_{s-1} r_{s-1}^m\right) \\
\cdots \Delta_2(x - x g_1 r_1^m, -x g_2 r_2^m) \cdot \Delta_1(x, -x g_1 r_1^m).
\end{aligned}$$

The s factors in this product are obtained by substitution of variables, hence $U(x)$ is invertible over $kM[x]$. Furthermore,

$$U(x) \cdot A(x) = A\left(x - \sum_{i=1}^{s} x g_i r_i^m\right) = A(0).$$

But $A(0)$ is a matrix over kM, so that the projective module it represents is free, and we can find a free basis by hypothesis. This completes the proof. □

This algorithm is needed as a subroutine in the next result, which represents the induction step in our main algorithm.

Proposition 18. *Suppose that M is a toric monoid and there is a QS-algorithm for M, then there is a QS-algorithm for the monoid ring $k[M \times \mathbf{Z}]$.*

Proof and algorithm. Let P be a finitely generated projective module over $k[M \times \mathbf{Z}]$. Represent $k[M \times \mathbf{Z}]$ as $kM[x,x^{-1}]$. Let S, respectively T, be the set of monic polynomials in $k[x]$, respectively $k[x^{-1}]$. Proposition 19 below implies that it is sufficient to find free bases for P_S and P_T. But $k[M \times \mathbf{Z}]_S = k(x)M$, so we can find a free basis for P_S by hypothesis. Similarly, $k[M \times \mathbf{Z}]_T = k(x^{-1})M \cong k(x)M$. (The last isomorphism follows from the fact that k is a field.) Therefore it is sufficient to give an algorithm for the following result.

Proposition 19. *Let P be a finitely generated projective $kM[x,x^{-1}]$-module. If $P \otimes k(x^{-1})$ is free, then P is free.*

To begin the proof, let U be a base change matrix with entries in $k(x^{-1})M$ which induces an isomorphism between $P \otimes k(x^{-1})$ and a free $k(x^{-1})M$-module, which can be found by hypothesis. Let $f \in k[x^{-1}]$ be a common denominator for the entries of U. Then P_f is free over $kM[x,x^{-1}]_f$, with the same matrix U inducing an isomorphism to a free module. Choose $n \geq 0$, such that $f = x^{-n}g$ with $g \in kM[x]$ and $g(0) = 1$. Consider the commutative square

$$\begin{array}{ccc} kM[x] & \longrightarrow & kM[x,x^{-1}] \\ \downarrow & & \downarrow \\ kM[x]_g & \longrightarrow & kM[x,x^{-1}]_g = kM[x,x^{-1}]_f. \end{array} \tag{3}$$

In order to continue the proof of Proposition 19, we need the following result.

Lemma 20. *Let R be a domain, and $f,g \in R$ such that $fR+gR = R$. Then the square*

$$\begin{array}{ccc} R & \longrightarrow & R_f \\ \downarrow & & \downarrow \\ R_g & \longrightarrow & R_{gf} \end{array}$$

is isomorphic to a pullback square.

Proof. We need to show that

$$R \cong \left\{ \left(\frac{a}{s}, \frac{b}{t} \right) \in R_f \times R_g \mid \frac{a}{s} = \frac{b}{t} \text{ in } R_{fg} \right\}.$$

Since R is a domain, we have that $ta = sb$. Since f and g are comaximal, so are any of their powers. Let $xs + yt = 1$, and define $r = xa + yb$. Then $sr = sxa + syb = sxa + tya = a$, so that $r = a/s$ in R_f. Likewise $r = b/t$ in R_g. □

We will show that square (3) has the Milnor patching property. (In fact, it is a so-called localization square, or generalized Karoubi square; see [19, p. 219].)

Rewrite the matrix U over $kM[x,x^{-1}]_f$ so that all denominators are equal to $f = x^{-n}g$. Let $\alpha \in \mathbf{Z}$ be such that $x^\alpha \cdot U$ does not contain any occurrence of x^{-1} in its entries. Replace P by the projective module $x^\alpha P$, which is isomorphic to P as a $kM[x,x^{-1}]$-module. After inverting f, $x^\alpha P$ becomes isomorphic to a free module, with an isomorphism given by the matrix $x^\alpha U$. This matrix has common denominator g and numerators in $kM[x]$, hence is a matrix over $kM[x]_g$. Let F be the free $kM[x]_g$-module given by the columns of the matrix $(x^\alpha U)^{-1}$. Then F becomes EQUAL to $x^\alpha P$ upon extending coefficients to $kM[x,x^{-1}]_g$. Presentation matrices of $x^\alpha P$ and F are

$$\operatorname{diag}(x^\alpha)A \quad \text{and} \quad \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$$

respectively, where I stands for an identity matrix of the appropriate size. The matrices become equal over $kM[x,x^{-1}]_g$, hence they lift to a matrix B over $kM[x]$, which presents a projective module Q that becomes equal to $x^\alpha P$ over $kM[x,x^{-1}]$. In particular, if Q is free, then it follows that P is free also.

It is therefore sufficient to give a constructive proof of the following result.

Lemma 21. *If all projective modules over kM are free, then the same is true for* $kM[x]$.

The key ingredient in the proof is Gubeladze's version of Roberts' Theorem, applied to our situation.

Theorem 22 (Gubeladze [8, Theorem 2.3]). *Let* $(R, \mathcal{M})$ *be a local ring, and A an R-algebra. Let P be a finitely generated A-module, and S a multiplicative set of A which is regular on A and P. Let n be a nonnegative integer. Suppose further that*

(i) *for every* $f \in S$, A/fA *is a finitely generated R-module;*

(ii) *the map* $\mathrm{SL}_n(A_S) \longrightarrow \mathrm{SL}_n(\overline{A_S})$ *is onto (where the bar denotes reduction modulo the maximal ideal* $\mathcal{M}$ *of R), and the group of units* $U(\overline{A_S})$ *is generated by the images of* $U(\bar{A})$ *and* $U(A_S)$;

(iii) *A_S contains a subalgebra B such that $A_S = A + B$ and $\mathcal{M}B \subset J(B)$ (the Jacobson radical of B)*;
(iv) *$P_S \cong A_S^n$ and $\bar{P} \cong \bar{A}^n$.*
Then $P \cong A^n$.

Algorithm 4 (Algorithm for Lemma 21)

Input: A toric monoid M, so that there exists a QS-algorithm for the monoid ring of M over all fields, and a finitely generated projective $kM[x]$-module P of rank t, with presentation

$$kM[x]^n \xrightarrow{C} kM[x]^m \longrightarrow P \longrightarrow 0.$$

Output: An $m \times m$ invertible matrix U over $kM[x]$ such that

$$U \cdot C = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

By Quillen's patching theorem it is enough to find such a matrix U for $P_{\mathcal{M}}$ for all maximal ideals $\mathcal{M}$ of kM. Let $R = kM_{\mathcal{M}}$ and $A = R[x]$. Let $S \subset A$ be the multiplicative set of monic polynomials in x with coefficients in k. Then we have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ \downarrow & & \downarrow \\ \bar{A} & \longrightarrow & \bar{A}_S, \end{array}$$

where

$$\bar{A} = A/\mathcal{M}A = k'[y], \quad A_S = (kM_{\mathcal{M}}[x])_S = k(x)M_{\mathcal{M}}, \quad \bar{A}_S = k'(y),$$

with $k' = kM/\mathcal{M}$, a field extension of k. The map

$$\mathrm{SL}_t(A_S) = \mathrm{SL}_t(k(x)M_{\mathcal{M}}) \longrightarrow \mathrm{SL}_t(\bar{A}_S) = \mathrm{SL}_t(k'(y))$$

is surjective, since $k'(y)$ is a field, so $\mathrm{SL}_t(k'(y)) = \mathrm{E}_t(k'(y))$, the subgroup generated by all elementary matrices, and the right vertical map is surjective. Since A_S is a local ring with quotient field $k'(y)$, the corresponding map on unit groups is surjective. Thus, Condition (ii) of Roberts' Theorem is satisfied, and so is (i).

Since $(P_{\mathcal{M}})_S = (P_S)_{\mathcal{M}}$ (subsequently denoted by P_S), we obtain an isomorphism to a free module by hypothesis, given by the commutative diagram

$$\begin{array}{ccccccc} A_S^n & \xrightarrow{C} & A_S^m & \longrightarrow & P_S & \longrightarrow & 0 \\ {\scriptstyle =}\downarrow & & {\scriptstyle U}\downarrow & & {\scriptstyle \cong}\downarrow & & \\ A_S^n & \xrightarrow{UC} & A_S^m & \longrightarrow & A_S^t & \longrightarrow & 0, \end{array}$$

where $U \in \mathrm{GL}_m(A_S)$ and

$$UC = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Since $\bar{A} = k'[y]$, we obtain a similar isomorphism by using the Euclidean algorithm to obtain a matrix $V \in \mathrm{GL}_m(\bar{A})$ such that

$$V\bar{C} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Let $u_1, \ldots, u_t$ be the A_S-basis of P_S that maps to the canonical basis of A_S^t under the isomorphism induced by U, i.e the image in P_S of the last t columns of U^{-1}. Similarly, let $\bar{v}_1, \ldots, \bar{v}_t$ in $\bar{P}$ form the $\bar{A}$-basis for $\bar{P}$ which maps to the canonical basis of $\bar{A}^t$ under the isomorphism induced by V. Lift the $\bar{v}_i \in \bar{P}$ to $v_1, \ldots, v_t$ in P, using Gröbner basis theory. Thus we obtain two free bases $\{\bar{u}_i\}$ and $\{\bar{v}_i\}$ for $\bar{P}_S = \overline{P_S}$. Compute a base change matrix $\overline{W} \in \mathrm{GL}_t(\bar{A}_S)$ which maps $\{\bar{v}_i\}$ to $\{\bar{u}_i\}$. If $\bar{a} = \det(\overline{W})$, a unit in $\bar{A}_S$, then

$$\overline{W} = \overline{W} \cdot \begin{pmatrix} \bar{a}^{-1} & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} \bar{a} & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

The product of the first two factors is in $\mathrm{SL}_t(\bar{A}_S)$, hence lifts to a matrix in $\mathrm{SL}_t(A_S)$. Likewise, the third factor lifts to an invertible matrix, since units lift. Thus, $\overline{W}$ lifts to an invertible matrix $W \in \mathrm{GL}_t(A_S)$. Now replace the basis $u_1, \ldots, u_t$ of P_S by the basis $W^{-1}u_1, \ldots, W^{-1}u_t$. Then for this new basis of P_S we have that $\bar{u}_i = \bar{v}_i$ for all i.

Let $P' = \sum A \cdot u_i$ be the A-submodule of P_S generated by the u_i. Since $\{u_i\}$ is a free A_S-basis of P_S, it follows that it forms a free A-basis for P'. Furthermore, the modules P and P' have the same image in $\bar{P}_S$, since $\bar{u}_i = \bar{v}_i$. We will now construct an explicit isomorphism between P and the free A-module P'.

Given an element $a = \sum \alpha_i u_i \in P_S$, we can write

$$\alpha_i = \frac{g_i}{h_i} = g_i' + \frac{g_i''}{h_i},$$

with $g_i, g_i', g_i'' \in A$, $h_i \in S$, and $\deg(g_i'') \leq \deg(h_i)$, where deg denotes the degree as a polynomial in x. Then

$$a = \sum \frac{g_i''}{h_i} \cdot u_i + \sum g_i' u_i.$$

Furthermore,

$$g_i' u_i = g_i' \frac{w_i}{f_i} = \frac{g_i}{f_i} w_i = \frac{q_i f_i + r_i}{f_i} w_i = q_i w_i + \frac{r_i}{f_i} w_i,$$

with $w_i \in P$ and $\deg(r_i) \leq \deg(f_i)$. We obtain a similar decomposition for $g_i'' u_i$.

Now we apply this decomposition to the elements $u_j - v_j$ to obtain

$$u_j - v_j = \sum \frac{g_i}{h_i} \cdot w_i + \sum g_i' w_i,$$

with $\deg(h_i) \geq \deg(g_i)$. It is shown in [9, p. 116] that the elements

$$v_j + \sum g_i' w_i, \quad j = 1, \ldots, t,$$

form a free A-basis of P. This completes Algorithm 4, needed to complete the proof of Lemma 21, hence that of Propositions 19 and 18. □

We now summarize the results of this section.

Algorithm 5 (Induction)

Input: A normal toric monoid M for which there exists a QS-algorithm, and a finitely generated projective module P over $k[M \times \mathbf{Z}]$, presented by a matrix A.

Output: An invertible matrix U over $k[M \times \mathbf{Z}]$ such that

$$U \cdot A = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Step 1: Represent $k[M \times \mathbf{Z}]$ as $kM[x, x^{-1}]$. Compute such a U over $k(x^{-1})M$, which is possible by the hypothesis on M.

Step 2: Construct a projective module Q over $kM[x]$ by Milnor patching applied to the generalized Karoubi square (3), as described after Lemma 20, which extends to P.

Step 3: Use the Quillen patching theorem algorithm (Proposition 17) to find a free basis for Q, with Algorithm 4 as the local loop to compute free bases for Q over the localizations at the various maximal ideals produced by the patching algorithm. Let V be the invertible matrix affecting the base change in the presentation of Q over $kM[x]$. Then the desired U is obtained from V by extension of scalars. □

Corollary 23. *The algorithm for Lemma 21 applied to the free monoid generated by $x_1, \ldots, x_r$ provides a QS-algorithm for the polynomial ring $k[x_1, \ldots, x_r]$.*

6. Pyramidal extensions and projective modules

Definition 24. A *pyramidal extension* is an extension of monoids $N \subset M$ such that

(i) M is a normal toric monoid.

(ii) There is a homomorphism $\delta : M \to \mathbf{Z}$ with $N = \{x \in M \mid \delta(x) \leq 0\}$.

(iii) There exists an element $v \in M$ such that $\delta(v) > 0$, and M is integral over $\langle N, v \rangle$, i.e. for each $x \in M$ there is $n > 0$ such that $x^n \in \langle N, v \rangle$.

A pyramidal extension will be called *nondegenerate* if there is an x such that $\delta(x) < 0$.

Note that if $N \subset M$ is a nondegenerate pyramidal extension then $\mathrm{rk}(N) = \mathrm{rk}(M)$ [19, p. 234].

Let $N \subset M$ be a nondegenerate pyramidal extension of toric monoids, and let P be a projective module over kM^*. The most complicated ingredient in the QS-algorithm is to construct a projective module over kN^* which extends to P under extension of scalars. This construction will then be applied to the admissible sequence constructed in Section 7, in order to complete the QS-Algorithm. We proceed by carrying out Milnor patching for the Karoubi square

$$\begin{array}{ccc} kN^* & \longrightarrow & kM^* \\ \downarrow & & \downarrow \\ kN^*_{\mathscr{M}^*} & \longrightarrow & kM^*_{\mathscr{M}^*}, \end{array}$$

where $\mathscr{M}^*$ is the maximal ideal of kN^* generated by $N^*\backslash\{1\}$, after showing that all projective modules over the lower right-hand ring are free. Thus, we need to prove

Proposition 25. *Let $N \subset M$ be a nondegenerate pyramidal extension of normal toric monoids, and let $\mathscr{M}^*$ be the maximal ideal of kN^* generated by $N^*\backslash\{1\}$. If P is a finitely generated projective kM^*-module, then one can find an explicit isomorphism from $P_{\mathscr{M}^*}$ to a free $kM^*_{\mathscr{M}^*}$-module.*

The proof will proceed by induction on the rank of M. If $\mathrm{rk}(M) = 1$, then $kM = kM^*$ is a polynomial ring in one variable over k, and P itself has a free basis, computed by using the Euclidean algorithm. So we may assume that $\mathrm{rk}(M) > 1$.

Let $N \subset M$ be a nondegenerate pyramidal extension of toric monoids, and P a finitely generated projective kM^*-module, with the free presentation

$$(kM^*)^n \xrightarrow{A} (kM^*)^p \longrightarrow P \longrightarrow 0,$$

where A is a matrix with entries in kM^*. Choose $z \in \mathrm{Int}(N)$, and find an integer m large enough so that all entries of A are contained in the homothetic submonoid $M^{(m)}$. Such an m exists by Lemma 14, and can be computed as in Lemma 13.

Then P is obtained by extension of scalars from the projective $k(M^{(m)})$-module Q defined by the same presentation matrix A. Furthermore,

$$N^{(m)} \subset M^{(m)}$$

is also a nondegenerate pyramidal extension [19, Lemma 10.1]. Let $\mathscr{M}'$ be the maximal ideal of $kN^{(m)}$ generated by $\mathrm{Int}(N^{(m)})$. Since $P_{\mathscr{M}^*}$ is obtained by extension of scalars from $Q_{\mathscr{M}'}$, it is sufficient to find an isomorphism from $Q_{\mathscr{M}'}$ to a free $kM^{(m)}$-module. That is, we need to prove the following:

Proposition 26. *Let $N \subset M$ be a nondegenerate pyramidal extension of normal toric monoids, and $\mathscr{M}$ the maximal ideal of kN generated by $N\backslash\{1\}$. If P is a finitely generated projective kM-module, then one can find an isomorphism from $P_{\mathscr{M}}$ to a free $kM_{\mathscr{M}}$-module.*

Proof and algorithm. Let $v \in M$ be as in (iii) of Definition 24. We first show that it is sufficient to find an isomorphism from P_v to a free $kM[v^{-1}]$-module. Observe that

$$kM[v^{-1}] \cong k[\langle M, v^{-1}\rangle],$$

and

$$\langle M, v^{-1}\rangle \cong M' \times \langle v\rangle \cong M' \times \mathbf{Z}.$$

Since $\mathrm{rk}(M') < \mathrm{rk}(M)$, we can apply the Induction Algorithm 5 to the monoid $M' \times \mathbf{Z}$. Therefore the proof of Proposition 26 will be complete if we can show the following result.

Proposition 27. *With hypotheses as in Proposition* 26, *if P_v is free, then P_M is free.*

Proof and algorithm. The proof proceeds by applying Roberts' Theorem to the ring $R = kN_M$ and the R-algebra $A = kM_M$, similar to the proof of Lemma 21. First we define a grading on the algebra A.

Suppose $N \subset M$ is a pyramidal extension with $w \in M$ such that $\delta(w) > 0$ and M is integral over $\langle N, w\rangle$. Then w lies on an extremal submonoid $E = \langle v\rangle$ of M [19, Lemma 8.3]. If $w = (a_1, \ldots, a_d) \in \mathbf{N}^d$, then $v = (a_1/a, \ldots, a_d/a)$ where $a = \gcd(a_1, \ldots, a_d)$. We now replace w by v, and call it a *vertex* of the pyramidal extension. Notice that if $M = \langle g_1, \ldots, g_s\rangle$, then by direct computation we can find $m > 0$ with each $g_i^m \in \langle N, v\rangle$. So, $x^m \in \langle N, v\rangle$ for each $x \in M$ implying $x^m = v^a y$ for some $a \geq 0$ and $y \in N$. For the rest of the discussion, such an m will be fixed.

Definition 28. (i) Let $x \in M$. Then $\deg(x) = \min\{a \geq 0 \mid x^m = v^a y \text{ for some } y \in N\}$.

(ii) Let $f = r_1 x_1 + \cdots + r_t x_t \in A$ where $r_i \in R$ and $x_i \in M$. Then $\deg(f) < p$ if and only if $\deg(x_i) < p$ for $i = 1, \ldots, t$.

(iii) If $f = v^a + g$ with $\deg(g) < \deg(v^a)$, we call f *monic*.

The following result provides us with a division algorithm in A.

Proposition 29 (Swan [19, Corollary 8.5]). *Let $f, g \in A$ with g monic. Then there are $q, r \in A$ with* $\deg(r) < \deg(g)$ *such that* $f = qg + r$.

Proof. Begin by initializing $q := 0$ and $r := f$. If $\deg(r) < \deg(g)$, we are done. Suppose $\deg(r) \geq \deg(g) = \deg(v^a) = am$. Write $r = r_1 x_1 + \cdots + r_t x_t$, where each $r_i \in R$ and $x_i \in M$. Then one of the x_i is such that $\deg(x_i) \geq \deg(v^a) = am$.

Claim 30. *We can write $x_i = v^a \tilde{x}_i$ where $\tilde{x}_i = x_i v^{-a} \in M$ with* $\deg(\tilde{x}_i) \leq \deg(x_i) - am$.

If we replace r with $r - r_i \tilde{x}_i g$ and q with $q + r_i \tilde{x}_i$, then $f = qg + r$. If $\deg(r)$ is still greater than or equal to $\deg(g)$, repeat the process. Since the degree of r strictly decreases with each pass, the process must eventually terminate with $f = qg + r$ and $\deg(r) < \deg(g)$. □

Proof of Claim 30. Since $N \subset M$ is a pyramidal extension, there exist $w_i \in N$ and $b \geq 0$ such that $x_i^m = v^b w_i$. But $\deg(x_i) \geq am$ so $x_i^m = v^{am}(v^{b-am}w_i)$ or $(x_i v^{-a})^m = v^{b-am}w_i$. Therefore, $\tilde{x}_i = x_i v^{-a} \in M$, since M is normal. Notice that $\deg(\tilde{x}_i) \leq b - am \leq \deg(x_i) - \deg(v^a)$. □

Let $S \subset A$ be the multiplicatively closed set of monic elements. Consider the commutative square

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ \downarrow & & \downarrow \\ \bar{A} & \longrightarrow & \bar{A}_S. \end{array}$$

Let

$$A^n \xrightarrow{C} A^p \longrightarrow P \longrightarrow 0$$

be a presentation for P. First we find isomorphisms from P_S and $\bar{P}$ to free modules. First of all, since $v \in S$ and there exists an isomorphism from P_v to a free A_v-module, we obtain an isomorphism from P_S to a free A_S-module by extension of scalars.

Now consider $\bar{P}$. If $x \in M$, then we can write $x^m = v^b y$ with $y \in N$. So we can write any element in A as a sum of a polynomial in v and an element which is nilpotent modulo $\mathcal{M}$. Hence $\bar{A}_{\text{red}} = k[v]$, and the canonical quotient map

$$\bar{A} = kM_{\mathcal{M}}/MkM_{\mathcal{M}} = kM/\langle N \setminus \{1\}\rangle \longrightarrow k[v] = kM/\langle M \setminus \langle v\rangle\rangle$$

is a split surjection. This can be seen by observing that $\langle v\rangle \subset M$ is extremal [19, Lemma 8.3], so we can use Lemma 16. Using the Euclidean algorithm, we can find an isomorphism from $\bar{P}_{\text{red}}$ to a free module, i.e. we can find an invertible matrix U_{red} over $\bar{A}_{\text{red}}$ such that

$$U_{\text{red}} \cdot \bar{C}_{\text{red}} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Lifting U_{red} to $\bar{A}$ via the splitting, we obtain an invertible matrix U over $\bar{A}$ such that

$$U \cdot \bar{C} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

(Recall that if a module Q is free modulo a nilpotent ideal, then it is free.) Thus, $\bar{P}$ is free. Furthermore, $\bar{P}$ and P_S have the same rank since A is a domain.

As in Roberts' theorem, we now proceed to construct a free module F over A from the free modules $\bar{P}$ and P_S, and an isomorphism from P to F. Let $x_1, \ldots, x_t$ be a free basis for P_S, for instance the inverse image of the canonical basis of A_S^t under the isomorphism constructed above. Furthermore, let $y_1, \ldots, y_t \in P$ be elements such that $\bar{y}_1, \ldots, \bar{y}_t$ is a free basis for $\bar{P}$. We first modify the basis for P_S so that $\bar{x}_i = \bar{y}_i$ in $\bar{P}_S$.

Both, $\{\bar{x}_i\}$ and $\{\bar{y}_i\}$ are free bases for $\bar{P}_S$ over $\bar{A}_S$. Let V be the invertible base change matrix which transforms the basis $\{\bar{x}_i\}$ to the basis $\{\bar{y}_i\}$, with $a = \det(V)$.

Lemma 31. *There exist units $b \in \bar{A}$ and $c \in A_S$ such that $a = b \cdot \bar{c}$ in $\bar{A}_S$.*

Proof and algorithm. Write $a = f/s$ with $s \in \bar{S}$ and $f \in \bar{A}$. It is sufficient to show that f is a product of a unit in $\bar{A}$ and an element of $\bar{S}$, which is done in the lemma below.

Observe that $\bar{A}$ has a graded structure,

$$\bar{A} = \bigoplus_i \bar{A}_i,$$

where $\bar{A}_i = \{\bar{a} \in \bar{A} \mid \delta(a) = i\}$ (see [19, p. 232]). Let $d = \delta(v)$.

Lemma 32. *With notation as above, $f = (1 + \eta)g$, where η is nilpotent and $g = v^n + a_{nd-1} + \cdots + a_0$, with $a_i \in \bar{A}_i$. Furthermore, $1 + \eta$ is a unit in $\bar{A}$, and $g \in \bar{A}$ lies in the image of S, so that $g \in \bar{A}_S$ is the image of a unit from A_S.*

Proof. Observe first that the image of S in $\bar{A}_{\text{red}} = k[v]$ consists of all monic polynomials, so that $(\bar{A}_S)_{\text{red}} = k(v)$. Since f divides an element of S, it follows that up to a unit of k, f maps to a monic polynomial in $k[v]$. Therefore, $f \equiv v^n + a_{nd-1} + \cdots + a_0$ modulo the nilradical of A. We now compute a decomposition

$$f = (1 + \eta)g,$$

with η nilpotent, and $g \in \bigoplus_{i=0}^{nd-1} A_i$. For this we need the following lemma.

Lemma 33. *Let B be the quotient of $\bar{A}$ modulo a nilpotent graded ideal, and let M be a finitely generated graded B-module, such that multiplication by $v \in \bar{A}_d$ induces an isomorphism $v : M_i \longrightarrow M_{i+d}$ for all $i \geq 0$. Let f be as above, and $z \in M$. Then we can write $z = fq + r$ with $q \in M$ and $r \in M_0 + \cdots + M_{nd-1}$. Moreover, q and r are unique.*

Proof. Let $f = f_0 + \cdots + f_m$, with f_i homogeneous of degree i. Then $f_{nd+1}, \ldots, f_m$ and $f_{nd} - v^n$ are nilpotent, and therefore generate a homogeneous nilpotent ideal J. Compute a nonnegative integer h such that $J^h = 0$. We proceed by induction on h. If $h = 0$, then we can simply use the usual division algorithm. Now let $h > 0$, and

$$N = \{x \in \bar{A} \mid v^k x \in J^{h-1} \text{ for some } k \geq 0\} = \bigcup_{k \geq 0} (J^{h-1} : v^k).$$

To compute N observe that this union is actually finite, since $(J^{h-1} : v^k) \subset (J^{h-1} : v^{k+1})$, so that we obtain an increasing sequence of ideals, and $\bar{A}$ is noetherian. Now observe that N is a graded ideal of $\bar{A}$, and multiplication by v induces an isomorphism $N_i \longrightarrow N_{i+d}$, since

$$N_i = N \cap \bar{A}_i \cong N \cap \bar{A}_{i+d} = N_{i+d}.$$

Therefore, the same is true for $\bar{A}/N$. Furthermore, $\bar{A}/N$ is a module over $\bar{A}/J^{h-1}$ and N is a module over $\bar{A}/J$. By induction the conclusion applies to N and to $\bar{A}/N$. So we can write

$$\bar{z} = \bar{f}\bar{q} + \bar{r}$$

in $\bar{A}/N$. Now lift back to $\bar{A}$ to obtain

$$z = fq + r + w,$$

with $w \in N$. Write $w = fq' + r'$, so that $z = f(q + q') + r + r'$. □

Now apply this lemma to $M = A$ and $z = v^n$. We obtain $v^n = fq + r$. Modulo the nilradical, f has the form $v^n + a_{nd-1} + \cdots + a_0$. Substitution gives that $\bar{q} = 0$ in $A/\mathrm{nil}(A)$, so that $q = 1 + \mu$ with μ nilpotent. Therefore q is a unit, with inverse $1 + \eta$. This completes the proof of Lemma 32. □

Returning to the proof of Proposition 27, we have now factored $a = \det(V) = b \cdot \bar{c}$ in A_S. We now change the basis $\{x_i\}$ for P_S by the invertible matrix

$$\begin{pmatrix} c^{-1} & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & & 1 \end{pmatrix},$$

and the basis $\{\bar{y}_i\}$ for $\bar{P}$ by a similar matrix, replacing c^{-1} by b^{-1}. Now the new base change matrix V over $\bar{A}_S$ has determinant one. But $\bar{A}_S$ is a local ring [19, p. 231], so $\mathrm{SL}_n(\bar{A}_S) = E_n(\bar{A}_S)$. An explicit factorization of a determinant one matrix into a product of elementary matrices can be obtained as follows. Use the fact that for an element x in a local ring, x or $1 - x$ is a unit to see that the first column must contain a unit. Now carry out Gauss–Jordan elimination by induction.

This shows that we can lift the base change matrix V to an invertible matrix $\tilde{V}$ over A_S. Now change the basis $\{x_i\}$ by the matrix $\tilde{V}^{-1}$. The resulting basis has the property that $\bar{x}_i = \bar{y}_i$ in $\bar{A}_S$ for all $i = 1, \ldots, t$.

We now proceed as in the proof of Lemma 21. Let $P' = \sum_i A \cdot x_i$ be the free A-submodule of P_S generated by the x_i. We will construct an isomorphism between P and P'. Let $a = \sum \alpha_i x_i \in A_S$. We can write $\alpha_i = f/g$ with g monic. Write $f = qg + r$ as in Proposition 29. Then

$$\frac{f}{g} = q + \frac{r}{g},$$

with $\deg(r) < \deg(g)$. Thus,

$$a = \sum \frac{r_i}{g_i} x_i + \sum q_i x_i.$$

For each i, write $x_i = w_i/h_i$ with $w_i \in P$ and $h_i \in S$, then

$$q_i x_i = q_i \frac{w_i}{h_i} = \frac{q_i' h_i + r_i'}{h_i} w_i = q_i' w_i + \frac{r_i'}{h_i} w_i,$$

with $\deg(r_i') < \deg(h_i)$. We obtain a similar decomposition for $r_i x_i$. Now apply these decompositions to the elements $x_j - y_j$ to obtain

$$x_j - y_j = \sum \frac{f_i}{g_i} w_i + \sum h_i w_i,$$

with $\deg(f_i) < \deg(g_i)$ and $h_i \in A$. It is shown in [19, p. 232; 9, p. 116] that the elements

$$x_j + \sum h_i w_i, \qquad j = 1, \ldots, t,$$

form a free A-basis for P. This completes the proof of Proposition 26. □

To complete the proof of Proposition 25, let P be a projective kM-module. Then we can find a free basis for $P_{\mathcal{M}}$, where $\mathcal{M}$ is the maximal ideal of kN generated by $N^* \setminus \{1\}$. The proof of Proposition 25 is now complete. □

Now consider the Karoubi square

$$\begin{array}{ccc} kN^* & \longrightarrow & kM^* \\ \downarrow & & \downarrow \\ kN^*_{\mathcal{M}^*} & \longrightarrow & kM^*_{\mathcal{M}^*}. \end{array}$$

Let P be a projective module over kM^*, and assume that we can find a free basis for projective modules over kN^*. We have just completed an algorithm for finding a free basis of $P_{\mathcal{M}^*}$ over $kM^*_{\mathcal{M}^*}$. Now use the Patching Algorithm 2 to construct a projective module Q over kN^* which extends to P. By hypothesis we can find a free basis for Q, thereby obtaining a free basis for P.

We summarize the results of this section.

Algorithm 6 (Local Algorithm)

Input: A nondegenerate pyramidal extension $N \subset M$ of normal toric monoids, and a finitely generated projective module P over kM^*, presented by a matrix A with entries in kM^*.

Output: An invertible matrix U over $kM^*_{\mathcal{M}^*}$ such that

$$U \cdot A = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

We proceed by induction on the rank of M. If $\mathrm{rk}(M) = 1$, then $kM = kM^*$ is a polynomial ring in one variable and one can find a free basis for P by using the Euclidean algorithm. So we may assume that $\mathrm{rk}(M) > 1$.

Step 1: Compute homothetic submonoids $N^{(m)} \subset M^{(m)}$ so that the entries of A are contained in $M^{(m)}$. Hence P can be viewed as a module over $kM^{(m)}$. Replace M by $M^{(m)}$, similarly for N.

Step 2: In this step we compute a free basis for the $kM_{\mathcal{M}}$-module P (Proposition. 26). Let v be a vertex of the extension $N \subset M$. View P as a module over $kM[v^{-1}]$.

Step 2.1: Find a free basis for P over $kM[v^{-1}]$ as follows. Observe that

$$kM[v^{-1}] \cong k[\langle M, v^{-1}\rangle],$$

and

$$\langle M, v^{-1}\rangle \cong M' \times \langle v\rangle \cong M' \times \mathbf{Z}.$$

Since $\mathrm{rk}(M') < \mathrm{rk}(M)$, we can compute free bases for projective kM'-modules inductively. Now use the induction algorithm 5 on the monoid $M' \times \mathbf{Z}$ to find a free basis for P over $kM[v^{-1}]$.

Step 2.2: Now use the algorithm of Proposition 27 to compute a free basis for P over $kM_{\mathcal{M}}$, with resulting base change matrix U'.

Step 3: Extending scalars to the original monoid ring $kM^*_{\mathcal{M}^*}$, we obtain the desired base change matrix $U = U'$. □

Algorithm 7 (Extension)

Input: A normal toric monoid M and a nondegenerate pyramidal extension $N \subset M$, as well as a projective module P over kM^*, presented by a matrix A with entries in kM^*.

Output: A projective module Q over kN^*, presented by a matrix B with entries in kN^*, together with an isomorphism $Q \cong P$ over kM^*.

Consider the Karoubi square

$$\begin{array}{ccc} kN^* & \longrightarrow & kM^* \\ \downarrow & & \downarrow \\ (kN)^*_{\mathcal{M}^*} & \longrightarrow & kM^*_{\mathcal{M}^*}, \end{array}$$

where $\mathcal{M}^*$ is the maximal ideal of kN^* generated by $N^* \backslash \{1\}$.

Step 1: View P as a module over $kM^*_{\mathcal{M}^*}$ by extension of scalars. Now use the Local Algorithm to compute a free basis for P over this ring.

Step 2: Use the Patching Algorithm 3 to construct a projective module Q over kN^* which extends to P. □

7. Admissible sequences

Let M be a normal toric monoid.

Definition 34. A sequence of submonoids

$$M = M_0, M_1, \ldots, M_n$$

of M is an *admissible sequence* if each M_i is a normal toric monoid, and for each i, either

(i) $M_{i+1} \subset M_i$ is a nondegenerate pyramidal extension, or

(ii) $M_i \subset M_{i+1}$.

A sequence will be called *weakly admissible* if we do not require the pyramidal extensions to be nondegenerate.

The objective of this section, Algorithm 9, is to construct an admissible sequence of submonoids starting with a normal toric monoid M and ending with a free monoid F contained in M^*, with $\mathrm{gp}(F) = \mathrm{gp}(M)$. The construction will proceed by induction on the rank of M. Before describing the details, we give an overview.

To begin, by using Lemma 10, we find a free monoid F contained inside M^* with $\mathrm{gp}(F) = \mathrm{gp}(M)$ with which the admissible sequence will end. Then, applying Proposition 35, which uses the extremal submonoids of M, we find an admissible sequence

$$M = M_0, M_1, \ldots, M_k \subsetneq M^*.$$

After obtaining a submonoid M_k which lies entirely within M^*, we find by means of Lemma 37 a homothetic transformation of M such that some homothetic submonoid $M^{(m)}$ lies strictly between M_k and M; thus we can extend to the admissible sequence

$$M = M_0, M_1, \ldots, M_k, M^{(m)}.$$

Since homothetic transformations behave well with respect to nondegenerate pyramidal extensions,

$$M = M_0, M_1, \ldots, M_k, M^{(m)}, M_1^{(m)}, \ldots, M_k^{(m)}$$

is also an admissible sequence. By repeatedly applying the homothetic transformation and normalizing, we can continue to extend the sequence:

$$M, \ldots, M_k, M^{(m)}, \ldots, M_k^{(m)}, (M^{(m)})^{(m)} = (M^{(m)})^2, \ldots, (M_k^{(m)})^2, (M^{(m)})^3, \ldots$$

where $(M^{(m)})^i$ denotes the normalization of the image $(\theta_m)^i(M)$. If we choose the homothetic transformation θ_m so that its center lies in $\mathrm{Int}(F)$ for the chosen free monoid F, then after a sufficient number s of iterations, we have $(M^{(m)})^s \subset F^*$. Consequently, we obtain the desired admissible sequence,

$$M = M_0, M_1, \ldots, M_k, M^{(m)}, \ldots, M_k^{(m)}, (M^{(m)})^2, \ldots, (M^{(m)})^s, F.$$

Proposition 35 (Swan [19, Corollary 11.8]). *Let M be a normal toric monoid which is not free. Then one can find an admissible sequence*

$$M = M_0, M_1, \ldots, M_k$$

such that $M_k \subsetneq M^*$.

Proof and algorithm

Step 1: Compute the proper extremal submonoids $E_1, \ldots, E_p$ of M using Lemma 8. Initialize $i := 0$.

Step 2: Set $i := i + 1$ and $E := E_i$. Since $\mathrm{rk}(E) \not\leq \mathrm{rk}(M)$, by the Induction Hypothesis 1, there is an admissible sequence

$$E = E_0, E_1, \ldots, E_n,$$

with E_n a free submonoid of E. Extend the sequence to the weakly admissible sequence

$$E, E_1, \ldots, E_n = \langle x_1, \ldots, x_s \rangle, E_{n+1} = \langle x_2, \ldots, x_s \rangle, \ldots, E_m = \{1\}. \tag{4}$$

Step 3: We now use (4) to form an admissible sequence for M. Notice that at each stage of (4), either $E_i \supset E_{i+1}$ is a pyramidal extension or $E_i \subset E_{i+1}$. Initialize $j := 0$.

Step 3.1: If $E_j \supset E_{j+1}$ is a pyramidal extension, we can construct a submonoid M_{j+1} such that $M_j \supset M_{j+1}$ is a nondegenerate pyramidal extension.

If the pyramidal extension $E_j \supset E_{j+1}$ is nondegenerate, it follows from the definition of nondegenerate pyramidal extension that E_{j+1} contains an extremal submonoid D such that $D \cap \mathrm{Int}(E_j) \neq \emptyset$. Compute generators for D using Lemma 8. Using linear algebra, determine a hyperplane $H = \{z \in \mathbf{R}^d \mid c \cdot z = 0\}$, where $c = (c_1, \ldots, c_d) \in \mathbf{Z}^d$, passing through the generators of D. Choose the signs on the vector c so that $c \cdot x \geq 0$ for all $x \in E_{j+1}$. Define $\delta : M \to \mathbf{Z}$ by $\delta(x) = c \cdot x$.

If the pyramidal extension $E_j \supset E_{j+1}$ is degenerate, it follows from the definition of pyramidal extension that E_{j+1} is an extremal submonoid of E_j. Use Lemma 8 to find generators for E_{j+1} and determine a hyperplane $H = \{z \in \mathbf{R}^d \mid c \cdot z = 0\}$ containing these generators with c chosen so that $c \cdot x \geq 0$ for all $x \in E_j$. Define $\delta : M \to \mathbf{Z}$ by $\delta(x) = c \cdot x$.

Once δ has been defined, use Lemma 8 to find generators for E_j and then find a hyperplane $H = \{y \in \mathbf{R}^d \mid d \cdot y = 0\}$ passing through these generators. Choose the signs on d so that $d \cdot x \geq 0$ for all $x \in M$. Set $\theta : M \to \mathbf{Z}$ where $\theta(x) = d \cdot x$.

Now define $\delta_k : M \to \mathbf{Z}$ as $\delta_k = \delta - k\theta$. Let $\{g_1, \ldots, g_r\}$ be the subset of generators of M_i not contained in E_i. By solving a system of r linear inequalities in the variable k, find a k such that $\delta_k(g_j) < 0$ for $1 \leq j \leq r$. Set $M_{i+1} = \{x \in M_i \mid \delta_k(x) \leq 0\}$. Then one can verify that $M_{i+1} \subset M_i$ is a nondegenerate pyramidal extension. Notice that $M_{i+1} \cap E_i = E_{i+1}$, and generators for M_{i+1} can be found by using a Hilbert basis algorithm.

Step 3.2: If $E_j \subset E_{j+1}$, put M_{j+1} equal to the normalization of $\langle M_j, E_{j+1}\rangle$. Generators for M_{j+1} can be found using Lemma 9.

Step 3.3: Set $j := j+1$. If $j = m$, proceed to Step 4. If $j < m$ and $E_j \supset E_{j+1}$ is a pyramidal extension, go to Step 3.1. If $j < m$ and $E_j \subset E_{j+1}$, go to Step 3.2.

Step 4: If $i < p$, return to Step 2. Once $i = p$, we have the desired admissible sequence. □

Example 36. We demonstrate Proposition 35 applied to the two-dimensional monoid

$$\begin{aligned} M &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\cdot \begin{pmatrix} -4 & 2 \\ 1 & -3 \end{pmatrix} \leq (0,0)\right\} \\ &= \langle (3,2),(1,1),(1,2),(1,3),(1,4)\rangle. \end{aligned}$$

The proper extremal submonoids of M are $E_1 = \langle (3,2)\rangle$ and $E_2 = \langle (1,4)\rangle$. So, E_1, $\{(0,0)\}$ and E_2, $\{(0,0)\}$ are weakly admissible sequences.

First, put $\delta : E_1 \to \mathbf{Z} : (x,y) \mapsto x$. Then $\{(0,0)\} = \{x \in E_1 \mid \delta(x,y) \leq 0\}$ as desired. Define $\phi : M \to \mathbf{N}$ as $(x,y) \mapsto -2x+3y$. Notice that $-2x+3y=0$ is the equation of the line corresponding to E_1 with the signs chosen so that $\phi(x,y) > 0$ for all $(x,y) \in M$. Then $\delta_k = (2k+1)x - 3ky$. We want to find $k \geq 1$ such that

$$\begin{aligned} \delta_k(1,1) &= -k+1 < 0, \\ \delta_k(1,2) &= -4k+1 < 0, \\ \delta_k(1,3) &= -7k+1 < 0, \\ \delta_k(1,4) &= -10k+1 < 0. \end{aligned}$$

By inspection, one can see that $k=2$ works. Thus, if we set

$$\begin{aligned} M_1 &= \{(x,y) \in M \mid \delta_2(x,y) = 5x - 6y \leq 0\} \\ &= \langle (6,5),(1,1),(1,2),(1,3),(1,4)\rangle, \end{aligned}$$

then the sequence M, M_1 is admissible.

Next, to continue the sequence, consider E_2. Define $\delta : E_2 \to \mathbf{Z}$ by $(x,y) \mapsto y$ and $\phi : M_1 \to \mathbf{N}$ by $(x,y) \mapsto 4x - y$. Then setting $\delta_4 = -16x + 5y$ yields an admissible sequence M, M_1, M_2 where

$$\begin{aligned} M_2 &= \{(x,y) \in M_1 \mid -16x + 5y \leq 0\} \\ &= \langle (6,5),(1,1),(1,2),(1,3),(5,16)\rangle \subsetneq M^*. \end{aligned}$$

Lemma 37 (Swan [19, Lemmas 9.2 and 9.3]). *Let M be a normal toric monoid and let N be a submonoid such that $N \subsetneq M^*$. Then there exists a homothetic submonoid $M^{(m)}$ with $N \subsetneq M^{(m)} \subsetneq M$.*

Proof. Let $\theta_m : M \to M$ be any homothetic transformation with center $z \in \mathrm{Int}(N)$. First, we claim that $M^{(i)} \subset M^{(i+1)}$ for all $i \geq 1$. Let $x \in M^{(i)}$. Then

$$\begin{aligned}\theta_i(x)^{i+1} &= x^{i(i+1)} z^{\psi(x)(i+1)} \\ &= x^{i(i+1)} z^{\psi(x)i} z^{\psi(x)} \\ &= \theta_{i+1}(x)^i z^{\psi(x)} \in M^{(i+1)}.\end{aligned}$$

Next, we claim that $\bigcup M^{(i)} = M^*$. Clearly, $\bigcup M^{(i)} \subset M^*$. Let $x \in \mathrm{Int}(M)$. By definition, $x^k = yz$ for some $k \in \mathbf{N}$ and $y \in M$. Set $i = \psi(y)$. Then $\theta_i(y) = y^i z^i = x^{ki} \in M^{(i)}$. But $M^{(i)}$ is normal, so $x \in M^{(i)}$. Consequently, since $N \subsetneq M^*$ and M^* is not finitely generated, there must be an $m \in \mathbf{N}$ with $N \subsetneq M^{(m)} \subsetneq M$. □

Algorithm 8 (Algorithm for Lemma 37)

Input: A normal toric monoid $M = \langle g_1, \ldots, g_t \rangle$ and submonoid $N \subsetneq M^*$.

Output: A homothetic submonoid $M^{(m)}$ with $N \subsetneq M^{(m)} \subsetneq M$.

Step 1: If N is finitely generated, set z equal to the product of all the generators of N. If N is not finitely generated, let z be any generator of N such that $z \in \mathrm{Int}(N)$. Define $\psi : M \to \mathbf{N}$ by $\psi(x) = x_1 + \cdots + x_d$ where $x = (x_1, \ldots, x_d) \in M$. Let $\theta_m : M \to M$ be the homothetic transformation with center z defined by $\theta_m(x) = x^m z^{\psi(x)}$. Initialize $m := 0$.

Step 2: Set $m := m + 1$. Using Lemma 13, compute generators for $M^{(m)}$. If $N \subsetneq M^{(m)} \subsetneq M$, we are done; otherwise repeat Step 2. This process must terminate by the proof of Lemma 37 above. □

Example 38. Continuing with the previous example, we apply Lemma 37 to

$$\begin{aligned}M &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -4 & 2 \\ 1 & -3 \end{pmatrix} \leq (0,0)\right\} \\ &= \langle (3,2),(1,1),(1,2),(1,3),(1,4)\rangle, \\ N &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -16 & 5 \\ 5 & -6 \end{pmatrix} \leq (0,0)\right\} \\ &= \langle (6,5),(1,1),(1,2),(1,3),(5,16)\rangle, \\ F &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix} \leq (0,0)\right\} \\ &= \langle (1,1),(1,2)\rangle.\end{aligned}$$

Let $z = (1,1) + (1,2) = (2,3)$ and define $\psi : M \to \mathbf{Z}$ by $(x,y) \mapsto x + y$. Then $\theta_m : M \to M$ is defined by $\theta_m(x,y) = m(x,y) + (x+y)(2,3)$. Notice $\theta_m(3,2) = (10+3m, 15+2m)$ and $\theta_m(1,4) = (10+m, 15+4m)$. Recall we want $N \subsetneq M^{(m)} \subsetneq M^*$. So, set $m = 22$, the smallest m such that

$$\frac{2}{3} < \frac{2m+15}{3m+10} < \frac{5}{6}$$

and

$$\frac{16}{5} < \frac{15+4m}{10+m} < 4.$$

Thus, we have extended our admissible sequence to

$$\begin{aligned}
M &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -4 & 2 \\ 1 & -3 \end{pmatrix} \leq (0,0)\right\} \\
&= \langle (3,2),(1,1),(1,2),(1,3),(1,4)\rangle, \\
M_1 &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -4 & 5 \\ 1 & -6 \end{pmatrix} \leq (0,0)\right\} \\
&= \langle (6,5),(1,1),(1,2),(1,3),(1,4)\rangle, \\
M_2 &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -16 & 5 \\ 5 & -6 \end{pmatrix} \leq (0,0)\right\} \\
&= \langle (6,5),(1,1),(1,2),(1,3),(5,16)\rangle, \\
M^{(22)} &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -103 & 59 \\ 32 & -76 \end{pmatrix} \leq (0,0)\right\},
\end{aligned}$$

which by Lemma 39 below, can be extended further to the admissible sequence

$$M, M_1, M_2, M^{(22)}, M_1^{(22)}, M_2^{(22)}.$$

Lemma 39. *Let M be a normal toric monoid and $N \subset M$ a nondegenerate pyramidal extension. Let θ_m be a homothetic transformation with center $z \in \mathrm{Int}(N)$. Then $N^{(m)} \subset M^{(m)}$ also forms a nondegenerate pyramidal extension.*

Proof. Assume $N \subset M$ is a nondegenerate pyramidal extension with $\delta : M \to \mathbf{Z}$ such that $N = \{x \in M \mid \delta(x) \leq 0\}$ and $v \in M \backslash N$ with M integral over $\langle v, N\rangle$. Then one can verify that $N^{(m)} \subset M^{(m)}$ forms a nondegenerate pyramidal extension with respect to $\delta\theta_m$ and v. □

Lemma 40. *Let $M = \langle g_1, \ldots, g_t\rangle$ be a normal toric monoid and let $F \subset M^*$ be a free monoid with $\mathrm{gp}(F) = \mathrm{gp}(M)$. Let $\theta_m : M \to M$ be a homothetic transformation with center $z \in \mathrm{Int}(F)$. Then after a finite number s of iterations, $(M^{(m)})^s \subset F^*$, where $(M^{(m)})^s$ is the normalization of $(\theta_m)^s(M)$.*

Proof. This result follows directly from Lemma 14. □

Example 41. We now apply Lemma 40 to the above example. Recall

$$\begin{aligned}
M &= \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -4 & 2 \\ 1 & -3 \end{pmatrix} \leq (0,0)\right\} \\
&= \langle (3,2),(1,1),(1,2),(1,3),(1,4)\rangle,
\end{aligned}$$

$$M^{(22)} = \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -103 & 59 \\ 32 & -76 \end{pmatrix} \leq (0,0)\right\},$$

$$F = \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix} \leq (0,0)\right\}$$

$$= \langle (1,1),(1,2)\rangle,$$

$$z = (2,3).$$

We want p large enough so that $(3,2) + p(2,3), (1,4) + p(2,3) \in \mathrm{Int}(F)$, i.e.

$$1 < \frac{2+3p}{3+2p} \quad \text{and} \quad \frac{4+3p}{1+2p} < 2.$$

The smallest such p is $p = 3$. If we set $s = pm = 3(22) = 66$, then

$$(M^{(22)})^{66} = \left\{(x,y) \in \mathbf{N}^2 \mid (x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \leq (0,0)\right\} \subset F,$$

where

$a = -8853803609322864800478421182048227632384771108443008831030103366567517827048965249648291865537 1,$

$b = 8853795649068786488773666953670414156230792401783290900608227416038648233037846949977354737396 3,$

$c = 5902529106003511273898318931050640524794865150078907612001838952270953889690044916706413636907 4,$

$d = -5902537066257589585603073159428454000948843856738625542423714902799823483701163216377350765048 2.$

Consequently,

$$M, M_1, M_2, M^{(22)}, M_1^{(22)}, M_2^{(22)}, (M^{(22)})^2, (M_1^{(22)})^2, (M_2^{(22)})^2, \ldots, (M^{(22)})^{66}, F$$

is an admissible sequence beginning with M and ending with F.

Algorithm 9 (Forming an admissible sequence)

Input: A normal toric monoid $M = \langle g_1, \ldots, g_t\rangle$.

Output: An admissible sequence

$$M = M_0, \ldots, M_n = F,$$

where $F \subset M^*$ is a free monoid with $\mathrm{gp}(F) = \mathrm{gp}(M)$.

Step 1: Using Lemma 10, find a free monoid $F \subset M^*$ with $\mathrm{gp}(F) = \mathrm{gp}(M)$.

Step 2: Apply Proposition 35 to form an admissible sequence $M = M_0, M_1, \ldots, M_k$ with $M_k \subset M^*$.

Step 3: Construct a homothetic submonoid $M^{(m)}$ with center $z \in \mathrm{Int}(F)$ such that $M_k \subsetneq M^{(m)} \subsetneq M$ by using Lemma 37.

Step 4: By Lemma 39, extend to an admissible sequence

$$M = M_0, M_1, \ldots, M_k, M^{(m)}, M_1^{(m)}, \ldots, M_k^{(m)}.$$

Step 5: By direct calculation, find a $p \geq 0$ such that $z^p g_i \in \mathrm{Int}(F)$ for $i = 1, \ldots, t$. Set $s = pm$. Then, by Lemma 40, extending to

$$M = M_0, M_1, \ldots, M_k, M^{(m)}, M_1^{(m)}, \ldots, M_k^{(m)}, (M^{(m)})^2 \ldots, (M^{(m)})^s, F,$$

yields the desired admissible sequence. □

8. The algorithm

In this section we summarize the algorithm with the steps in their natural order.

Algorithm 10 (QS-Algorithm)

Input:

(i) A toric monoid M, described in terms of generators and relations. The monoid ring kM can then be described as the quotient of a polynomial ring over k modulo the binomial ideal of defining relations [7, Theorem 7.11];

(ii) a finitely generated projective kM-module P of rank t, presented as the cokernel of a matrix A:

$$(kM)^n \xrightarrow{A} (kM)^m \longrightarrow P \longrightarrow 0.$$

Output: An invertible matrix U with entries in kM such that

$$U \cdot A = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix},$$

where I denotes an identity matrix of size $(m - t) \times (m - t)$. The last $m - t$ rows of U form a free basis for P.

The algorithm proceeds by induction on the rank of M. If $\mathrm{rk}(M) = 1$, then kM is a polynomial ring in one variable, so we can find U by using the Euclidean algorithm.

Step 1: Compute the normalization $\tilde{M}$ of M. Since $\tilde{M}^* = M^*$ [19, Lemma 6.6], we can replace M by $\tilde{M}$ and assume from now on that M is normal.

Step 2: Compute all extremal submonoids $E_1, \ldots, E_r$ of M (Lemma 8), listed in order of increasing rank, as in Section 4.

Step 3: Carry out the Reduction Algorithm 3 to compute a projective module Q over kM^* and an isomorphism from Q to P over kM.

Step 4: Find a free monoid $F \subset M^*$ and an admissible sequence

$$M = M_0, M_1, \ldots, M_s = F$$

(Admissible Sequence Algorithm 9).

Step 5: Set $i = 0$, and $Q_0 = Q$. *While* $i \leq s - 1$ *do*:

If $M_i \subset M_{i+1}$, then set $Q_{i+1} = Q_i$, viewed as a kM_{i+1}-module by extension of scalars.

Otherwise, apply the Extension Algorithm 7 to the nondegenerate pyramidal extension $M_{i+1} \subset M_i$ to construct a projective module Q_{i+1} and an isomorphism from Q_{i+1} to Q_i over kM_i.

Set $i := i + 1$.

Step 6: Apply the Logar–Sturmfels algorithm to find a free basis for the module Q_s over the polynomial ring kF.

Step 7: Extend the resulting base change matrix in the free presentation of Q_s to kM to obtain the desired matrix U. □

Corollary 42. *There is a QS-algorithm over Laurent polynomial rings.*

Proof. Let $M = \mathbf{Z}^r$, then $R = kM = k[x_1^{\pm 1}, \ldots, x_r^{\pm 1}]$. Consider the commutative diagram

$$\begin{array}{ccc} k[x_1^{\pm 1}, \ldots, x_{r-1}^{\pm 1}] & \longrightarrow & R \\ \downarrow & & \downarrow \\ k & \longrightarrow & k[x_r^{\pm 1}]. \end{array}$$

It is a Milnor square, and the right vertical map, which sends the first $r-1$ variables to 1, is a split epimorphism. The Induction Algorithm applies to the lower right-hand corner, viewed as the monoid ring of the monoid $\{1\} \times \mathbf{Z}$. The Patching Algorithm 1 applies to carry out an induction argument. □

Remark 43. The same type of argument allows the extension of the algorithm to monoids which do contain nontrivial units, alternatively, to all subrings of Laurent polynomial rings which are generated by monomials and are seminormal [19, Theorem 1.1′].

Acknowledgements

The authors would like to thank Bernd Sturmfels for suggesting the problem, and for helpful discussions. The first author would like to thank Joseph Gubeladze for several helpful conversations. Finally, thanks are due to several referees for their comments.

References

[1] W. Adams and P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Math. Vol. 3 (Amer. Math. Soc., Providence, RI, 1994).

[2] D.F. Anderson, Projective modules over subrings of $k[X, Y]$ generated by monomials, Pacific J. Math. 79 (1978) 5–17.

[3] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms, Undergraduate Texts in Math., (Springer, New York, 1992).

[4] N. Fitchas (working group), Algorithmic aspects of Suslin's proof of Serre's conjecture, Comp. Complexity 3 (1993) 31–55.

[5] N. Fitchas and A. Galligo, Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen–Suslin) pour le Calcul Formel, Math. Nachr. 149 (1990) 231–253.

[6] W. Fulton, Introduction to Toric Varieties, Annals of Mathematics Studies, Vol. 131 (Princeton University Press, Princeton, NJ, 1993).

[7] R. Gilmer, Commutative Semigroup Rings, Chicago Lectures in Mathematics (The University of Chicago Press, Chicago, 1984).

[8] I. DZH. Gubeladze, Anderson's conjecture and the maximal monoid class over which projective modules are free, Math. USSR Sb. 63 (1989) 165–180.
[9] T.Y. Lam, Serre's Conjecture, Lecture Notes in Math, Vol. 635 (Springer, New York, 1978).
[10] A. Logar, Computational aspects of the coordinate ring of an algebraic variety, Comm. Algebra 18 (1990) 2641–2662.
[11] A. Logar and B. Sturmfels, Algorithms for the Quillen–Suslin theorem, J. Algebra 145 (1992) 231–239.
[12] H. Park, A computational theory of Laurent polynomial rings and multidimensional fir systems, Ph.D. Thesis, UC Berkeley, Berkeley, CA, 1995.
[13] H. Park and C. Woodburn, An algorithmic proof of Suslin's stability theorem for polynomial rings, J. Algebra 178 (1995) 277–298.
[14] D. Quillen, Projective modules over polynomial rings, Invent. Math. 36 (1976) 167–171.
[15] J.-P. Serre, Faisceaux algébriques cohérents, Ann. Math 61 (1955) 191–278.
[16] B. Sturmfels, Algorithms in Invariant Theory (Springer, New York, 1993).
[17] A.A. Suslin, Projective modules over a polynomial ring are free, Sov. Math. Dokl. 17 (1976) 1160–1164.
[18] R.G. Swan, Projective modules over Laurent polynomial rings, Trans. Amer. Math. Soc. 237 (1978) 111–120.
[19] R.G. Swan, Gubeladze's proof of Anderson's conjecture, in: D. Haile and J. Osterburg, eds., Azumaya Algebras, Actions and Modules, Contemporary Mathematics 124 (Amer. Math. Soc., Providence, RI, 1992) 215–250.
[20] D.C. Youla and P.F. Pickel, The Quillen–Suslin theorem and the structure of n-dimensional elementary polynomial matrices, IEEE Trans. Circuits and Systems 31 (1994) 513–517.
[21] G.M. Ziegler, Lectures on Polytopes, Grad. Texts in Math Vol. 152 (Springer Verlag, New York, 1995).