Armenian Journal of Mathematics
Volume 13, Number 1, 2021, 1–21

Saturation of finitely-generated submodules of free modules over Prüfer domains

F. Ben Amor and I. Yengui

Abstract. We propose to give an algorithm for computing the $\mathbf{R}$-saturation of a finitely-generated submodule of a free module E over a Prüfer domain $\mathbf{R}$. To do this, we start with the local case, that is, the case where $\mathbf{R}$ is a valuation domain. After that, we consider the global case ($\mathbf{R}$ is a Prüfer domain) using the dynamical method. The proposed algorithm is based on an algorithm given by Ducos, Monceur and Yengui in the case $E = \mathbf{R}[X]^m$ which is reformulated here in a more general setting in order to reach a wider audience. The last section is devoted to the case where $\mathbf{R}$ is a Bézout domain. Particular attention is paid to the case where $\mathbf{R}$ is a principal ideal domain ($\mathbb{Z}$ as the main example).

Key Words: Valuation domains, Prüfer domains, Echelon form, Saturation, Abelian groups
Mathematics Subject Classification 2010: 13C99, 13P99, 20K10, 20K15

Introduction

We propose an algorithm for computing the $\mathbf{R}$-saturation of a finitely-generated submodule of a free module E over a Prüfer domain $\mathbf{R}$. To do this, we start with the local case, that is, the case where $\mathbf{R}$ is a valuation domain. The proposed algorithm is based on an algorithm given in [3] with $E = \mathbf{R}[X]^m$ which is reformulated here in a more general setting in order to reach a wider audience (i.e., not only those interested in polynomials over a Prüfer domain). We also give a "compact" formula expressing a necessary and sufficient condition for a finitely-generated submodule of a free module over a valuation domain $\mathbf{V}$ to be $\mathbf{V}$-saturated in terms of its dimensions as a vector space over the quotient and residue fields of $\mathbf{V}$. After that, we consider the global case ($\mathbf{R}$ is a Prüfer domain) using the dynamical method [1] and being inspired by the notion of dynamical Gröbner bases [4, 7]. The last section is devoted to the case where $\mathbf{R}$ is a Bézout domain. Particular attention is paid to the case where $\mathbf{R}$ is a principal ideal domain (supposed to be $\mathbb{Z}$ in order to lighten the notation). Our approach is based on the solution of the problem over $\mathbb{Q}$ and also over a finite number of localizations $\mathbb{Z}_{p\mathbb{Z}}$, p being an "essential prime number" of considered module.

1 V-saturation with V being a valuation domain

Everywhere in this section we suppose $\mathbf{V}$ to be a valuation domain. Recall that a *valuation domain* is an integral ring $\mathbf{V}$ equipped with a divisibility test in which every two elements are comparable under division, i.e., given a, $b \in \mathbf{V}$, $a \mid b$ or $b \mid a$. In particular, a valuation ring $\mathbf{V}$ is local with maximal ideal $\mathrm{Rad}(\mathbf{V})$. A valuation domain does not need to be a principal ideal domain (PID).

Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$. A vector $u = \sum_i u_i e_i \in E$ is said to be *primitive* if it has an invertible coefficient u_i. Let $u = \sum_i u_i e_i$ be a primitive vector in E. The greatest i such that $u_i \in \mathbf{V}^\times$ will be called the *index* of u and will be denoted by $\mathrm{index}(u)$. We also denote by $\mathrm{primc}(u) := u_{\mathrm{index}(u)}$ (the *primitive coefficient* of u). For example, if $\mathbf{V} = \mathbb{Z}_{2\mathbb{Z}} = \{a/b \in \mathbb{Q} \mid (a, b) \in \mathbb{Z} \times \mathbb{Z} \text{ and } b \text{ is odd}\}$ and $u = -4e_1 + 2e_2 + 2e_3 + 3e_4 + 4e_5$, we have $\mathrm{index}(u) = 4$, and $\mathrm{primc}(u) = 3$.

For $u = \sum_i u_i e_i \in E \setminus \{0\}$, denote by u_{i_0} the right-most coefficient of u dividing all the others. The primitive vector u/u_{i_0} is called *the primitive version* of u and denoted by $\mathrm{Prim}(u)$.

Let $u = \sum_i u_i e_i$ and $v = \sum_i v_i e_i$ be two primitive vectors in E. By the result of *the reduction of v by u* we mean the vector $w = v + \alpha\, u = \sum_i w_i e_i \in E$ where $\alpha \in \mathbf{V}$ is chosen such that $w_{\mathrm{index}(u)} = 0$, that is, $\alpha = -\mathrm{primc}(u)^{-1} v_{\mathrm{index}(u)}$. For example, if $u = -4e_1 + 2e_2 + 2e_3 + 3e_4 + 4e_5$ and $v = 4e_1 + 5e_4 + e_5$ then the term $5e_4$ in v disappears with $\alpha = -5/3$ as follows

$$v \xleftarrow{u} v - (5/3)u = (32/3)e_1 - (10/3)e_2 - (10/3)e_3 - (17/3)e_5.$$

By an *operation of type* 1, we mean the operation of type

$$v \ \leftarrow v - \mathrm{primc}(u)^{-1} v_{\mathrm{index}(u)}\, u,$$

where $u, v \in E$ and u is primitive. By an *operation of type* 2, we mean the operation of type

$$v \ \leftarrow \mathrm{Prim}(v),$$

for some $v \in E \setminus \{0\}$.

Let $L := [L_1,\, L_2, \ldots]$ be a list of vectors in E where $L_j = \sum_i L_{j,i} e_i$, $L_{j,i} \in \mathbf{V}$. We say that L is *primitive triangular* if all the L_j's are primitive and for each $1 \leq j < \ell$, we have $L_{\ell,\,\mathrm{index}(L_j)} = 0$. We say that L is *in an echelon form* if all the L_j's are primitive and the $\mathrm{index}(L_j)$'s are pairwise different. It is not difficult to see that if L is primitive triangular then it is in an echelon form.

Let $\mathbf{R}$ be a domain with quotient field $\mathbf{K}$, and consider a family $(s_j)_{j\geq 1}$ of vectors in a free $\mathbf{R}$-module E. By *the* $\mathbf{R}$*-saturation* of $M := \sum_{j=1}^{\infty} \mathbf{R} s_j$ in E we mean

$$\mathrm{Sat}(M) := \{ s \in E \mid \ \alpha\, s \in E \ \text{ for some } \alpha \in \mathbf{R} \setminus \{0\} \} = (E \otimes_{\mathbf{R}} \mathbf{K}) \cap E.$$

If $\mathrm{Sat}(M) = M$, we say that M is $\mathbf{R}$-*saturated* in E, or, if there is no ambiguity, that M is *saturated*.

The following three lemmas are cornerstones in the saturation algorithm we will give.

Lemma 1 *Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$. For any two primitive vectors $u = \sum_i u_i e_i$ and $v = \sum_i v_i e_i \in E$ such that* $\mathrm{index}(u) \neq \mathrm{index}(v)$*, the result $w = \sum_i w_i e_i$ of the reduction of v by u is primitive and* $\mathrm{index}(w) = \mathrm{index}(v)$*.*

Proof. In order to lighten the notation, let us consider the following two cases.

If $\mathrm{index}(u) = 2$ and $\mathrm{index}(v) = 1$, then

$$w = (v_1 + \alpha\, u_1)e_1 + (v_3 + \alpha\, u_3)e_3 + (v_4 + \alpha\, u_4)e_4 + \cdots$$

for some $\alpha \in \mathrm{Rad}(\mathbf{V})$. Thus, $w_1 \in \mathbf{V}^{\times}$ and $w_i \in \mathrm{Rad}(\mathbf{V})$ for $i \geq 2$.

If $\mathrm{index}(u) = 1$ and $\mathrm{index}(v) = 2$, then

$$w = (v_2 + \beta\, u_2)e_2 + (v_3 + \beta\, u_3)e_3 + \cdots$$

for some $\beta \in \mathbf{V}$. Hence, $w_1 = 0$, $w_2 \in \mathbf{V}^{\times}$, and $w_i \in \mathrm{Rad}(\mathbf{V})$ for $i \geq 3$.

In general cases, the proof can be done analogously. □

Lemma 2 *Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$. If $S = [s_1,\, s_2, \ldots]$ is a primitive triangular list of vectors in E, then $\sum_{j\geq 1} \mathbf{V} s_j$ is $\mathbf{V}$-saturated.*

Proof. Denote by $\mathbf{K}$ the quotient field of $\mathbf{V}$, $M := \sum_{j\geq 1} \mathbf{V} s_j$, and let $s \in \mathrm{Sat}(M)$. Then there exist $a_1 \ldots, a_r \in \mathbf{K}$ such that

$$s = a_1 s_1 + \cdots + a_r s_r.$$

For each $1 \leq j \leq r$, by identifying the coefficient in $\mathrm{index}(s_j)$ and denoting $c_j = \mathrm{primc}(s_j)$, we obtain:

$$\begin{cases} c_1 a_1 \in \mathbf{V}, \\ b_{2,1}a_1 + c_2 a_2 \in \mathbf{V}, \\ \vdots \\ b_{r,1}a_1 + b_{r,2}a_2 + \cdots + b_{r,r-1}a_{r-1} + c_r a_r \in \mathbf{V}, \end{cases}$$

with $b_{i,j} \in \mathbf{V}$. Since $c_1, \ldots, c_r \in \mathbf{V}^\times$, this triangular system yields that $a_1, \ldots, a_r \in \mathbf{V}$, as desired. □

Lemma 3 *Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$ and $S = [s_1,\ s_2, \ldots]$ be a list of primitive vectors in E which is in an echelon form. Then we can transform S into a primitive triangular list $S' = [s'_1, s'_2, \ldots]$ of vectors in E only by means of operations of type* 1.

Proof. As in the gaussian algorithm, this can be done with operations of type 1 and 2. But Lemma 1 guaranties that all vectors computed when reducing S to S' are primitive, and thus, there is no need of operations of type 2. □

Let E be a $\mathbf{V}$-module, $\mathbf{K}$ be the quotient field of $\mathbf{V}$, and $\mathbf{k} = \mathbf{V}/\mathrm{Rad}(\mathbf{V})$ be the residue field of $\mathbf{V}$. For a list $S = [s_1, \ldots, s_r]$ of vectors in E, denote by $\langle S \rangle_{\mathbf{V}}$ the $\mathbf{V}$-module generated by $s_1, \ldots, s_r$. We denote by $\langle S \rangle_{\mathbf{K}}$ (respectively, $\langle S \rangle_{\mathbf{k}}$) the $\mathbf{K}$-vector space (respectively, the $\mathbf{k}$-vector space) generated by $s_1, \ldots, s_r$ in $E \otimes_{\mathbf{V}} \mathbf{K}$ (respectively, by $\bar{s}_1, \ldots, \bar{s}_r$ in $E \otimes_{\mathbf{V}} \mathbf{k}$, where for $u = \sum_i u_i e_i \in E$, $\bar{u} := \sum_i \bar{u}_i e_i$, $\bar{u}_i$ denoting the class of u_i modulo $\mathrm{Rad}(\mathbf{V})$),

$$\dim_{\mathbf{K}} S := \dim_{\mathbf{K}} \langle S \rangle_{\mathbf{K}}, \text{ and } \dim_{\mathbf{k}} S := \dim_{\mathbf{k}} \langle S \rangle_{\mathbf{k}}.$$

Now we reach the main result the proposed saturation algorithm will be based on.

Proposition 1 *Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$, and let $S = [s_1,\ s_2, \ldots]$ be a list of primitive vectors in E. If S is in an echelon form, then $\sum_{j=1}^{\infty} \mathbf{V} s_j$ is $\mathbf{V}$-saturated.*

Proof. By virtue of Lemma 3, we can transform the list S into a primitive triangular list $S' = [s'_1, s'_2, \ldots]$ only with the help of operations of type 1, and, thus, $\sum_{j=1}^{\infty} \mathbf{V} s_j = \sum_{j=1}^{\infty} \mathbf{V} s'_i$. On the other hand, using Lemma 2, we infer that $\sum_{j=1}^{\infty} \mathbf{V} s'_j$ is $\mathbf{V}$-saturated. □

Example 1 Let E be a free $\mathbf{V}$-module with a countable basis $(e_1, e_2, \ldots)$, and consider a primitive vector $u = \sum_{i \geq 1} u_i e_i$ in E. Then, obviously, the list $[u^{(0)} = u, u^{(1)} = \sum_{i \geq 1} u_i e_{i+1}, \ldots, u^{(j)} = \sum_{i \geq 1} u_i e_{i+j}, \ldots]$ is in an echelon form, and, thus, $\sum_{j=0}^{\infty} \mathbf{V} u^{(j)}$ is $\mathbf{V}$-saturated.

The following algorithm will be the cornerstone of our saturation algorithm.

Algorithm 1 (Algorithm for reduction modulo a list in an echelon form)
Input: A free $\mathbf{V}$-module E with a countable basis $(e_1, e_2, \ldots)$, a nonzero vector $u \in E$, and a finite list $S = [s_1, \ldots, s_n]$ of vectors in E in an echelon form.
Output: A reduction $v = \mathrm{PrimRed}(u; S) = \mathrm{PrimRed}(u; s_1, \ldots, s_n)$ of u modulo S such that $[S, v]$ becomes in an echelon form and $\mathrm{Sat}(\langle s_1, \ldots, s_n, u\rangle_{\mathbf{V}}) = \mathrm{Sat}(\langle s_1, \ldots, s_n, v\rangle_{\mathbf{V}})$.

```
    $v := \mathrm{Prim}(u)$
    FOR $j$ FROM 1 TO $n$ DO
    $v := \mathrm{Prim}(v - \mathrm{primc}(s_j)^{-1} v_{\mathrm{index}(s_j)} s_j)$
(reduction of $v$ by $s_j$ such that $v_{\mathrm{index}(s_j)}$ becomes zero)
```

Now we give the following saturation algorithm for finitely-generated sub-$\mathbf{V}$-modules of a free $\mathbf{V}$-module with a countable basis.

Algorithm 2 (Saturation Algorithm for a finitely-generated sub-$\mathbf{V}$-module of a free $\mathbf{V}$-module with a countable basis)
Input: A free $\mathbf{V}$-module E with a countable basis $(e_1, e_2, \ldots)$, a finite list $S = [s_1, \ldots, s_n]$ of nonzero vectors in E.
Output: A generating list $V = [v_1, \ldots, v_r] = \mathrm{Echel}(S)$ for $\mathrm{Sat}(\mathbf{V}s_1 + \cdots + \mathbf{V}s_n)$.

```
    $v_1 := \mathrm{Prim}(s_1)$
    IF $n \geq 2$ THEN FOR $i$ from 2 to $n$ DO
        $v_i := \mathrm{PrimRed}(\mathrm{Prim}(s_i); v_1, \ldots, v_{i-1})$    (use Algorithm 1; disregard
zero vectors)
```

Example 2 Consider the list $[s_1 = 8e_1 + 2e_2 + 8e_3 + 8e_4,\ s_2 = e_2 + 2e_3 - 2e_4]$ of vectors in a free $\mathbb{Z}_{2\mathbb{Z}}$-module E with basis $(e_1, \ldots, e_4, \ldots)$. Executing Algorithm 2, we obtain

$$\mathrm{Sat}(\mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2) = (\mathbb{Q}\, s_1 + \mathbb{Q}\, s_2) \cap E = \mathbb{Z}_{2\mathbb{Z}}\, v_1 + \mathbb{Z}_{2\mathbb{Z}}\, v_2,$$

with

$$\begin{aligned} v_1 := \mathrm{Prim}(s_1) = \frac{1}{2} s_1 = 4e_1 + e_2 + 4e_3 + 4e_4, \quad \mathrm{index}(v_1) = 2; \\ v_2 := \mathrm{PrimRed}(\mathrm{Prim}(s_2); v_1) = \mathrm{PrimRed}(s_2; v_1) = \mathrm{Prim}(s_2 - v_1) \\ = \mathrm{Prim}(-4e_1 - 2e_3 - 6e_4) = \frac{2}{3} e_1 + \frac{1}{3} e_3 + e_4. \end{aligned}$$

Remark 1 In fact, Algorithm 2 works in any free $\mathbf{V}$-module (not necessary with a countable basis). As a matter of fact, for any finite list $S = [s_1, \dots, s_n]$ of vectors in a free $\mathbf{V}$-module with basis $(e_i)_{i \in I}$, the s_j's depend only on a finite number of the e_i's.

Algorithm 2 allows us to give a new proof of the following classical result.

Theorem 1 *A finitely-generated submodule of a free module over a valuation domain $\mathbf{V}$ is $\mathbf{V}$-saturated if and only if it is a direct summand.*

Proof. The sufficiency is obvious. Let us prove the necessity. Let $S = [s_1, \dots, s_n]$ be a finite list of vectors in a free $\mathbf{V}$-module E with basis $(e_i)_{i \in I}$, and suppose that $M := \langle s_1, \dots, s_n \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated. First note that the s_j's depend only on a finite number of the e_i's, say, $e_{i_1}, \dots, e_{i_t}$. Set $J := \{i_1, \dots, i_t\} \subseteq I$, and let F be the free sub-$\mathbf{V}$-module of E with basis $(e_i)_{i \in J}$. Using Algorithm 2, we can compute a generating list $[v_1, \dots, v_r] = \mathrm{Echel}(S)$ for the $\mathbf{V}$-saturation M' of M in F. But since F is $\mathbf{V}$-saturated in E and M is $\mathbf{V}$-saturated in E, we have $M = M' = \langle v_1, \dots, v_r \rangle_{\mathbf{V}}$. It remains to note that $v_1, \dots, v_r$ can be completed into a free basis of E by adding all the e_i's with $i \in I \setminus \{\mathrm{index}(v_1), \dots, \mathrm{index}(v_r)\}$. □

The proof of Theorem 1 implies the following algorithm that, for a finitely-generated submodule M of a free module E over a valuation domain $\mathbf{V}$, computes a submodule N of E such that $\mathrm{Sat}(M) \oplus N = E$.

Algorithm 3 ($\mathbf{V}$-saturated finitely-generated submodule of a free module as a direct summand)
Input: A free $\mathbf{V}$-module E with basis $(e_i)_{i \in I}$, a finite list $S = [s_1, \dots, s_n]$ of nonzero vectors in E.
Output: A submodule N of E such that $\mathrm{Sat}(\mathbf{V}s_1 + \cdots + \mathbf{V}s_n) \oplus N = E$.

Let $e_{i_1}, \dots, e_{i_t}$ be the elements of the basis $(e_i)_{i \in I}$ on which the s_j's depend, and set $F := \mathbf{V}e_{i_1} + \cdots + \mathbf{V}e_{i_t}$. Using Algorithm 2, compute a generating list $V = [v_1, \dots, v_r] = \mathrm{Echel}(S)$ for the $\mathbf{V}$-saturation of $\mathbf{V}s_1 + \cdots + \mathbf{V}s_n$ in F.

Return $N := \sum_{i \in I \setminus \{\mathrm{index}(v_1), \dots, \mathrm{index}(v_r)\}} \mathbf{V}e_i$.

Example 3 For the case considered in Example 2, we have:

$$\mathrm{Sat}(\mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2) \oplus (\mathbb{Z}_{2\mathbb{Z}}e_1 + \mathbb{Z}_{2\mathbb{Z}}e_3 + \sum_{i \geq 5} \mathbb{Z}_{2\mathbb{Z}}e_i) = E.$$

The characterization of saturated finitely generated sub-$\mathbf{V}$-module of a free module E over a valuation domain $\mathbf{V}$ given in Theorem 1 is "quite satisfactory", but not enough, because it is not easy to test whether a submodule of E is a direct summand. Our goal now is to give a "compact" formula characterizing such submodules.

Lemma 4 *Let E be a $\mathbf{V}$-module, where $\mathbf{V}$ is a valuation domain of quotient field $\mathbf{K}$ and residue field $\mathbf{k}$. If S is a finite list of vectors in E, then $\dim_{\mathbf{K}} S \geq \dim_{\mathbf{k}} S$.*

Proof. Let $S = [s_1, \ldots, s_r]$, $d = \dim_{\mathbf{k}} L$, and suppose that $\bar{s}_1, \ldots, \bar{s}_d$ are $\mathbf{k}$-linearly independent. Then, necessarily, $s_1, \ldots, s_d$ are $\mathbf{K}$-linearly independent. To see this, let $\alpha_1, \ldots, \alpha_d \in \mathbf{V}$ be such that $\alpha_1 s_1 + \cdots + \alpha_d s_d = 0$. Since $\mathbf{V}$ is a valuation domain, there exists i_0, $1 \leq i_0 \leq d$, such that α_{i_0} divides all the α_i's. Note, that if $\alpha_{i_0} \neq 0$, then $\bar{s}_{i_0} \in \sum_{1 \leq i \leq d;\, i \neq i_0} \mathbf{k}\bar{s}_i$ and, thus, $\alpha_1 = \cdots = \alpha_d = 0$. Therefore, $\alpha_{i_0} = 0$, and hence, $\dim_{\mathbf{K}} L \geq d = \dim_{\mathbf{k}} L$. □

Now we give a necessary and sufficient condition for a finitely-generated submodule of a free $\mathbf{V}$-module to be $\mathbf{V}$-saturated using its corresponding dimensions as $\mathbf{K}$-vector space and $\mathbf{k}$-vector space.

Theorem 2 *Let S be a finite list of vectors in free $\mathbf{V}$-module E, where $\mathbf{V}$ is a valuation domain of quotient field $\mathbf{K}$ and residue field $\mathbf{k}$. Then $\langle S \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated if and only if $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S$.*

Proof. Let $S = [s_1, \ldots, s_r]$ and let $(e_i)_{i \in I}$ be a basis of E as a $\mathbf{V}$-module. Since the s_j's depend only on a finite number of the e_i's, we can suppose that E has a finite rank.

To prove sufficiency, we proceed by induction on r. For $r = 1$, two cases may arise. In the case $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S = 0$, we have $S = [0]$ and, of course, $\{0\}$ is $\mathbf{V}$-saturated as $\mathbf{V}$ is a domain. If $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S = 1$, then s_1 is necessarily primitive and, thus, $\mathbf{V}s_1$ is $\mathbf{V}$-saturated.

Suppose now that $r > 1$.

Case 1: s_1 is not primitive. Denote $S' = [s_2, \ldots, s_r]$. Necessarily, $s_1 \in \langle S' \rangle_{\mathbf{K}}$, because otherwise we would have

$$\dim_{\mathbf{k}} S' = \dim_{\mathbf{k}} S = \dim_{\mathbf{K}} S = 1 + \dim_{\mathbf{K}} S' \geq 1 + \dim_{\mathbf{k}} S'.$$

Since $\dim_{\mathbf{K}} S = \dim_{\mathbf{K}} S'$, $\dim_{\mathbf{k}} S = \dim_{\mathbf{k}} S'$, and $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S$, we infer that $\dim_{\mathbf{K}} S' = \dim_{\mathbf{k}} S'$. The $\mathbf{V}$-module $\langle S' \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated by the induction hypothesis. Now, since $s_1 \in \langle S' \rangle_{\mathbf{K}}$, there exist $\beta_1 \in \mathbf{V} \setminus \{0\}$ and $\beta_2, \ldots, \beta_r \in \mathbf{V}$ such that $\beta_1 s_1 = \beta_2 s_2 + \cdots + \beta_r s_r$, and hence, $s_1 \in \langle S' \rangle_{\mathbf{V}}$. It follows that $\langle S \rangle_{\mathbf{V}} = \langle S' \rangle_{\mathbf{V}}$, and, thus, $\langle S \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated as desired.

Case 2: s_1 is primitive. For $2 \leq j \leq r$, we set $v_j := s_j + \alpha_j\, s_1 = \sum_i v_{j,i} e_i$, where $\alpha_j \in \mathbf{V}$ is such that $v_{j,\mathrm{index}(s_1)} = 0$. Denoting by $L := [v_2, \ldots, v_r]$, we have $\langle S \rangle_{\mathbf{V}} = \mathbf{V}s_1 \oplus \langle L \rangle_{\mathbf{V}}$, $\dim_{\mathbf{K}} S = \dim_{\mathbf{K}} L + 1$, and $\dim_{\mathbf{k}} S = \dim_{\mathbf{k}} L + 1$. Since $\dim_{\mathbf{K}} S = \dim_{\mathbf{k}} S$, we have $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L$. Since $\langle L \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated (by the induction hypothesis), $\mathbf{V}s_1$ is saturated as well (by virtue of the case $r = 1$).

Let us prove the necessity. We can put S in an echelon form by means of operations of type 1 and 2. It is clear that an operation of type 1 does not affect the $\mathbf{V}$-module generated by the current list. Also, so does an operation of type 2 since $\langle S\rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated. Denoting by U the new list obtained after putting S in an echelon form, we get $\dim_{\mathbf{K}} S = \dim_{\mathbf{K}} U = \dim_{\mathbf{k}} U = \dim_{\mathbf{k}} S$. $\square$

Example 4 Let E be a free $\mathbb{Z}_{2\mathbb{Z}}$-module with basis $(e_1, \ldots, e_5, \ldots)$. Consider the list $[s_1 = e_1 + 2e_2 + 2e_5,\ s_2 = e_1 + 2e_3 + 2e_4]$ of vectors in E. Clearly, we have

$$\dim_{\mathbb{Q}}(\mathbb{Q}\, s_1 + \mathbb{Q}\, s_2) = 2 > \dim_{\mathbb{F}_2}(\mathbb{F}_2\, \bar{s}_1 + \mathbb{F}_2\, \bar{s}_2) = 1.$$

Thus, by Theorem 2, the $\mathbb{Z}_{2\mathbb{Z}}$-module $\mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2$ is not $\mathbb{Z}_{2\mathbb{Z}}$-saturated. From here it follows that $\{s_1,\ s_2\}$ is not a generating set for $\mathrm{Sat}(\mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2)$. Executing Algorithm 2, we find

$$\mathrm{Sat}(\mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2) = \mathbb{Z}_{2\mathbb{Z}}\, v_1 + \mathbb{Z}_{2\mathbb{Z}}\, v_2,$$

with

$$v_1 := \mathrm{Prim}(s_1) = s_1,\ v_2 := \mathrm{Prim}(s_2 - s_1) = -(1/2)(s_2 - s_1) = e_2 - e_3 - e_4 + e_5.$$

Finally, $\dim_{\mathbb{Q}}(\mathbb{Q}\, v_1 + \mathbb{Q}\, v_2) = 2 = \dim_{\mathbb{F}_2}(\mathbb{F}_2\, \bar{v}_1 + \mathbb{F}_2\, \bar{v}_2)$.

Theorem 2 implies an algorithm which, for a finitely-generated submodule M of a free $\mathbf{V}$-module E over a valuation domain $\mathbf{V}$ of quotient field $\mathbf{K}$ and residue field $\mathbf{k}$ such that $\dim_{\mathbf{K}} M > \dim_{\mathbf{k}} M$, exhibits a vector $u \in E$ witnessing that M is not saturated, i.e., $u \in \mathrm{Sat}(M) \setminus M$.

Algorithm 4 (Saturation test over a valuation domain and a witness for nonsaturation if so)
Input: A nonempty finite list S of nonzero vectors in a free $\mathbf{V}$-module E with basis $(e_i)_{i \in I}$.
Output: An answer to the question whether $\langle S\rangle_{\mathbf{V}}$ is saturated or not, and, in the case of negative answer, a vector $u \in \mathrm{Sat}(\langle S\rangle_{\mathbf{V}}) \setminus \langle S\rangle_{\mathbf{V}}$.

Since the $S[j]$'s [1] depend only on a finite number of the e_i's, we can suppose that E has a finite rank.

WHILE one of the entries of S is primitive and $\sharp(S) > 1$ DO

Consider a primitive element $S[j_0]$ in S. Using Algorithm 1, for each j, $1 \leq j \leq \sharp(S)$ and $j \neq j_0$, compute $v_j := \mathrm{PrimRed}(S[j]; S[j_0])$, and replace S with the list formed by the nonzero vectors among $v_1, \ldots, v_{j_0-1}, v_{j_0+1} \cdots, v_{\sharp(S)}$.

1. If none of the $S[j]$'s is primitive, then $\langle S\rangle_{\mathbf{V}}$ is not saturated and $\mathrm{Prim}(S[1]) \in \mathrm{Sat}(\langle S\rangle_{\mathbf{V}}) \setminus \langle S\rangle_{\mathbf{V}}$.

2. If $\sharp(S) = 1$ and $S[1]$ is primitive, then $\langle S\rangle_{\mathbf{V}}$ is saturated.

[1] $S[j]$ denotes the j^{th} entry of S; $S = [S[1], \ldots, S[\sharp(S)]]$.

Example 5 Denoting $M := \mathbb{Z}_{2\mathbb{Z}}\, s_1 + \mathbb{Z}_{2\mathbb{Z}}\, s_2$ in Example 4, we have

$$v_2 \in \mathrm{Sat}(M) \setminus M.$$

Our goal now is, given a list $[u, s_1, \ldots, s_n]$ of vectors in a free $\mathbf{V}$-module E, to present an algorithm to test whether $u \in \mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$ or not, and, in the case of positive answer, to express u as a linear combination of the generators of $\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$ computed with Algorithm 2.

Algorithm 5 (Saturation membership test over a valuation domain)
Input: A finite list $[u, s_1, \ldots, s_n]$ of vectors in a free $\mathbf{V}$-module E with basis $(e_i)_{i\in I}$, where $\mathbf{V}$ is a valuation domain of quotient field $\mathbf{K}$.
Output: An answer to the question whether u is in $\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$ or not; and, in the case of positive answer, a finite list $[v_1, \ldots, v_r]$ of vectors in E generating $\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$ as a $\mathbf{V}$-module and a list $[\alpha_1, \ldots, \alpha_r]$ of elements in $\mathbf{V}$ such that $u = \alpha_1 v_1 + \cdots + \alpha_r v_r$.

Since the s_j's depend only on a finite number of the e_i's, we can suppose that E has a finite rank.

1. Test if $u \in \mathbf{K}s_1 + \ldots + \mathbf{K}s_n$. If the answer is NO, then return NO. Else, continue.

2. Write u as a $\mathbf{K}$-linear combination of the s_j's.

3. Use Algorithm 2 to compute a finite list $[v_1, \ldots, v_r]$ of vectors in E generating $\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$ as a $\mathbf{V}$-module.

4. Write each s_j's $(1 \leq j \leq n)$ as a $\mathbf{K}$-linear combination of the v_t's $(1 \leq t \leq r)$ by tracing the computations done with Algorithm 2.

5. Write u as a $\mathbf{K}$-linear combination $u = \alpha_1 v_1 + \cdots + \alpha_r v_r$ of the v_t's (using 2. and 4.). Note that, by virtue of the proof of Lemma 2, the obtained $\mathbf{K}$-linear combination is a $\mathbf{V}$-linear combination if and only if $u \in \mathrm{Sat}(\langle s_1, \ldots, s_n \rangle)$. Thus, $\alpha_t \in \mathbf{V}$ for $1 \leq t \leq r$.

2 R-saturation with R being a Prüfer domain

We need first to recall the notion of comaximal monoids and Prüfer domains.

We say that S is a *multiplicative subset* (or a *monoid*) of a ring $\mathbf{R}$ if $1 \in S$ and for any $a, b \in S$, $a\, b \in S$. For example, for $a \in \mathbf{R}$, $a^{\mathbb{N}} := \{a^n;\ n \in \mathbb{N}\}$ is a monoid of $\mathbf{R}$. The localization of $\mathbf{R}$ at S will be denoted by $S^{-1}\mathbf{R}$ or $\mathbf{R}_S$. If S is generated by $a \in \mathbf{R}$, we denote $\mathbf{R}_S$ by $\mathbf{R}_a$ or $\mathbf{R}[1/a]$. Note here that $\mathbf{R}_a$ is isomorphic to the ring $\mathbf{R}[T]/(aT-1)$. We keep the same notation for the localization of an $\mathbf{R}$-module.

We say that elements $a_1, \ldots, a_k$ of a ring $\mathbf{R}$ are *comaximal* if $\langle a_1, \ldots, a_k \rangle = \mathbf{R}$. For example, for any $a \in \mathbf{R}$, a and $1 - a$ are comaximal. We say that monoids $S_1, \ldots, S_n$ of $\mathbf{R}$ are *comaximal* if any ideal of $\mathbf{R}$ meeting all the S_i's contains 1. In other words, if for any $a_1 \in S_1, \ldots, a_n \in S_n$ there exist $b_1, \ldots, b_n \in \mathbf{R}$ such that $\sum_{i=1}^n b_i a_i = 1$, that is, $a_1, \ldots, a_k$ are comaximal elements in $\mathbf{R}$. For example, if $a_1, \ldots, a_m$ are comaximal elements in $\mathbf{R}$, then the monoids $a_1^{\mathbb{N}}, \ldots, a_m^{\mathbb{N}}$ are comaximal.

A ring $\mathbf{R}$ is *Bézout* if each finitely-generated ideal is principal. A ring $\mathbf{R}$ is *arithmetical* if for any $x, y \in \mathbf{R}$, there exist $s, t, a, b \in \mathbf{R}$ such that

$$\left\{ \begin{array}{rcl} s\,x & = & a\,y, \\ b\,x & = & t\,y, \\ s+t & = & 1. \end{array} \right. \tag{1}$$

See [2] for detailed explanations about this characterization. Property (1) amounts to saying that each finitely-generated ideal becomes principal after localization at a finite family of comaximal monoids.

An integral domain is called a *Prüfer domain* if it is arithmetical. A Noetherian Prüfer domain is called a *Dedekind domain.*

Let E be a free $\mathbf{R}$-module over a Prüfer domain $\mathbf{R}$, and consider a finite list $S = [s_1, \ldots, s_n]$ of nonzero vectors in E. In this section, we give an algorithm computing a generating list for $\mathrm{Sat}(\mathbf{R}s_1 + \cdots + \mathbf{R}s_n)$.

As for dynamical Gröbner bases [4, 7], one can obtain a dynamical version of Algorithm 2 for Prüfer domains. This algorithm works like Algorithm 2 for valuation domains. The only difference is when it has to handle two incomparable (under division) elements a, b in $\mathbf{R}$. In this situation, one should first compute $\alpha, \beta, \gamma \in \mathbf{R}$ such that

$$\left\{ \begin{array}{l} \alpha b = \beta a, \\ \gamma b = (1-\alpha) a. \end{array} \right.$$

Now, the computations are pursued in $\mathbf{R}_\alpha$ (in which, $a \mid b$) and in $\mathbf{R}_{1-\alpha}$ (in which, $b \mid a$). At the end of the dynamical computations with Algorithm 2, we obtain a finite binary tree whose leaves are comaximal localizations $S_1^{-1}\mathbf{R}, \ldots, S_k^{-1}\mathbf{R}$ of $\mathbf{R}$. Over each localization $S_j^{-1}\mathbf{R}$, $1 \leq j \leq k$, we obtain a generating set $H_j = \{h_{j,1}, ..., h_{j,p_j}\}$ for $\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle_{S_j^{-1}\mathbf{R}})$. For each $1 \leq i \leq p_j$, there exists $d_{j,i} \in S_j$ such that $d_{j,i} h_{j,i} \in E$. Under these hypotheses, we have:

Theorem 3 *(Saturation over a Prüfer domain) For any* $\mathbf{R}$*-module,*

$$\mathrm{Sat}(\langle s_1, \ldots, s_n \rangle_{\mathbf{R}}) = \langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k} \rangle_{\mathbf{R}}.$$

Proof. It is clear that

$$\langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k} \rangle \subseteq \mathrm{Sat}(\langle s_1, \ldots, s_n \rangle_{\mathbf{R}}).$$

To prove the converse, let $h \in \mathrm{Sat}(\langle s_1, \ldots, s_n\rangle_{\mathbf{R}})$. It is also in $\mathrm{Sat}(\langle s_1, \ldots, s_n\rangle_{S_j^{-1}\mathbf{R}})$ for each $1 \leq j \leq k$. Hence, for some $d_j \in S_j$, $d_j h \in \langle d_{j,1}h_{j,1}, \ldots, d_{j,p_j}h_{j,p_j}\rangle_{\mathbf{R}}$. On the other hand, since $S_1, \ldots, S_k$ are comaximal multiplicative subsets of $\mathbf{R}$, there exist $\alpha_1, \ldots, \alpha_k \in \mathbf{R}$ such that $\sum_{j=1}^{k} \alpha_j d_j = 1$. From the fact that $h = \sum_{j=1}^{k} \alpha_j d_j h$, we infer that

$$h \in \langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k}\rangle_{\mathbf{R}}.$$

□

Example 6 Let $\theta = \sqrt{-5}$ and E be a free $\mathbb{Z}[\theta]$-module with basis $(e_1, e_2, \ldots)$. Consider the list $[s_1 = 3e_1 + (4+2\theta)e_2,\ s_2 = \theta e_1 + 3e_3]$ of vectors in E. Suppose that we want to compute a generating set for $\mathrm{Sat}(\langle s_1, s_2\rangle_{\mathbb{Z}[\theta]})$.

Note that the ring $\mathbb{Z}[\theta]$ is a Dedekind domain which is not a Bézout domain (and, thus, nor principal). Since $a := 3$ and $b := 4 + 2\theta$ are not comparable under division in $\mathbb{Z}[\theta]$, we have to find $\alpha, \beta, \gamma \in \mathbb{Z}[\theta]$ such that

$$\begin{cases} \alpha b = \beta a, \\ \gamma b = (1-\alpha)a. \end{cases}$$

Further, since the ring $\mathbb{Z}[\theta]$ has a $\mathbb{Z}$-basis (it is a rank 2 free $\mathbb{Z}$-module), α, β, γ can be computed by solving an underdetermined linear system over the integers. A solution is given by $\alpha = 5 + 2\theta$, $\beta = 6\theta$, $\gamma = -3$. Then we can open two branches:

$$\begin{tikzcd} & \mathbb{Z}[\theta] \arrow[dl] \arrow[dr] & \\ \mathbb{Z}[\theta]_{4+2\theta} & & \mathbb{Z}[\theta]_{5+2\theta} \end{tikzcd}$$

<u>Over $\mathbb{Z}[\theta]_{5+2\theta}$:</u>

$$[s_1, s_2] = \left[3\left(e_1 + \frac{6\theta}{5+2\theta}e_2\right), \theta e_1 + 3e_3\right] \to \left[e_1 + \frac{6\theta}{5+2\theta}e_2, \frac{10}{5+2\theta}e_2 + e_3\right]$$

(the list is in an echelon form without additional branching).

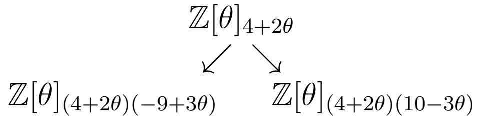
<u>Over $\mathbb{Z}[\theta]_{(4+2\theta)}$:</u>

$$[s_1, s_2] = \left[(4+2\theta)\left(\frac{3}{4+2\theta}e_1 + e_2\right), \theta e_1 + 3e_3\right] \to \left[\frac{3}{4+2\theta}e_1 + e_2, \theta e_1 + 3e_3\right]$$

Since θ and 3 are not comparable under division in $\mathbb{Z}[\theta]_{(4+2\theta)}$, we have to consider two comaximal localizations. We find $\alpha = 3(-3+\theta)$, $\beta = -5 - 3\theta$, $\gamma = -3(3+2\theta)$ as solutions to the following system over the integers:

$$\begin{cases} \alpha\theta = 3\beta, \\ \gamma\theta = 3(1-\alpha). \end{cases}$$

We then split the ring $\mathbb{Z}[\theta]_{(4+2\theta)}$ as follows:


$\mathbb{Z}[\theta]_{4+2\theta}$
$\mathbb{Z}[\theta]_{(4+2\theta)(-9+3\theta)}$
$\mathbb{Z}[\theta]_{(4+2\theta)(10-3\theta)}$

Over $\mathbb{Z}[\theta]_{(4+2\theta)(-9+3\theta)}$:

$$\left[\frac{3}{4+2\theta}e_1+e_2, \theta e_1+3e_3\right] \to \left[\frac{3}{4+2\theta}e_1+e_2, \frac{5+3\theta}{9-3\theta}e_1+e_3\right]$$

(the latter list is in an echelon).

Over $\mathbb{Z}[\theta]_{(4+2\theta)(10-3\theta)}$:

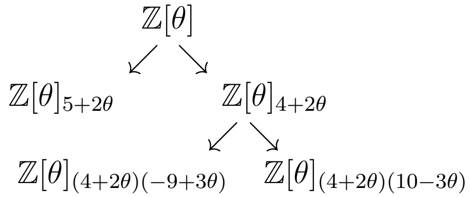
$$\left[\frac{3}{4+2\theta}e_1+e_2, \theta e_1+3e_3\right] \to \left[\frac{3}{4+2\theta}e_1+e_2, e_1+\frac{-9+3\theta}{10-3\theta}e_3\right]$$

(the latter list is in an echelon).

Finally, over $\mathbb{Z}[\theta]$:

$$\begin{aligned}\mathrm{Sat}(\langle s_1,s_2\rangle_{\mathbb{Z}[\theta]}) = \langle &(5+2\theta)e_1+6\theta e_2, 10e_2+(5+2\theta)e_3, 3e_1+(4+2\theta)e_2,\\ &(5+3\theta)e_1+(9-3\theta)e_3, (10-3\theta)e_1+(-9+3\theta)e_3\rangle.\end{aligned}$$

The dynamical evaluation of the problem of computing a generating set for $\mathrm{Sat}(\langle s_1,s_2\rangle_{\mathbb{Z}[\theta]})$ produced the following binary tree:


$\mathbb{Z}[\theta]$
$\mathbb{Z}[\theta]_{5+2\theta}$
$\mathbb{Z}[\theta]_{4+2\theta}$
$\mathbb{Z}[\theta]_{(4+2\theta)(-9+3\theta)}$
$\mathbb{Z}[\theta]_{(4+2\theta)(10-3\theta)}$

3 Z-saturation with Z being a Bézout domain

In this section we consider a Bézout domain $\mathbf{Z}$. Let E be a free $\mathbf{Z}$-module with a countable basis $(e_1,e_2,\ldots)$. For $u=\sum_i u_ie_i \in E\setminus\{0\}$, we denote by $\gcd(u)$ the greatest common divisor of all the nonzero u_i's and $\mathrm{Prim}(u) := (1/\gcd(u))\,u$ (we convene that $\mathrm{Prim}(0)=0$). To explain the dynamical version of Algorithm 2 over Bézout domains, it suffices to give the dynamical versions of type 1 and type 2 operations. This can be done as follows.

By a (dynamical) operation of type 2, we mean the operation of type

$$u \;\leftarrow \mathrm{Prim}(u), \qquad u \in E\setminus\{0\}.$$

Denoting by $d_1, \ldots, d_s$ the nonzero coefficients of $\mathrm{Prim}(u)$, we have $\gcd(d_1, \ldots, d_s) = 1$. Note that $\mathrm{Prim}(u)$ is a primitive vector (i.e., with one invertible coefficient) over each localization $E[1/d_i] := E \otimes_{\mathbf{Z}} \mathbf{Z}[1/d_i]$. A Bézout identity between the d_i's guarantees that the monoids $d_1^{\mathbb{N}}, \ldots, d_s^{\mathbb{N}}$ are comaximal. Such a vector will be simply called a *primitive* vector (a vector whose coefficients generate the whole ring).

Let $u = \sum_i u_i e_i$, $v = \sum_i v_i e_i \in E$ and suppose that u is primitive. To avoid redundancies, since the gcd of the elements of the set H formed by nonzero coefficients of u is 1, one can consider a minimal (for inclusion) subset $\{u_{i_1}, \ldots, u_{i_r}\}$ of H with $i_1 < i_2 < \cdots < i_r$ such that $\gcd(u_{i_1}, \ldots, u_{i_r}) = 1$. It is worth mentioning that the LLL method [6] provides an effective algorithm for finding a short basis of a given lattice and can be used for finding $u_{i_1}, \ldots, u_{i_r}$ [5].

By an operations of type 1, we mean the operation of type

$$v \ \leftarrow [u_{i_1} v - v_{i_1} u, \ldots, u_{i_r} v - v_{i_r} u].$$

At each localization $\mathbf{Z}[1/u_{i_j}]$, the vector

$$u_{i_j} v - v_{i_j} u = u_{i_j} \left(v - \frac{v_{i_j}}{u_{i_j}} u \right)$$

is, up to a unit, equal to the reduction $\tilde{v} = \sum_i \tilde{v}_i e_i \in E$ of v by u such that $\tilde{v}_{i_j} = 0$. Contrary to the local case (i.e., the case where the base ring is a valuation domain), a type 1 reduction may produce more than one vector if one wants to do all the reductions at once (i.e., globally over $\mathbf{Z}$) instead of doing them at each localization $\mathbf{Z}[1/u_{i_j}]$ separately.

In the particular case of two vectors, we infer the following result.

Proposition 2 *Let E be a free $\mathbf{Z}$-module with basis $(e_i)_{i \in I}$. Let $S = [u = \sum_i u_i e_i,\ v = \sum_i v_i e_i]$ be a list formed by two vectors in E with $u \neq 0$. Then*

$$\mathrm{Sat}_{\mathbf{Z}}(\langle u, v \rangle_{\mathbf{Z}}) = \langle \mathrm{Prim}(u),\ \mathrm{Prim}(u_{i_1} v - v_{i_1} u), \ldots, \mathrm{Prim}(u_{i_r} v - v_{i_r} u) \rangle_{\mathbf{Z}},$$

where $u_{i_1}, \ldots, u_{i_r}$ are nonzero coefficients of u.

Proof. Let us put "dynamically" the list $[u, v]$ in an echelon form by executing the dynamical version of Algorithm 2 explained above. One has first to replace u by its primitive version $\tilde{u} = \mathrm{Prim}(u) = (1/c)u$, where $c = \gcd(u)$. The obtained new list is then

$$[\tilde{u},\ \mathrm{Prim}((u_{i_1}/c)v - v_{i_1}\tilde{u}), \ldots, \mathrm{Prim}((u_{i_1}/c)v - v_{i_r}\tilde{u})]$$

with

$$\begin{aligned} \mathrm{Prim}\left(\frac{u_{i_j}}{c} v - v_{i_j} \tilde{u} \right) &= \mathrm{Prim}\left(\frac{1}{c} (u_{i_j} v - v_{i_j} u) \right) \\ &= \frac{1}{\gcd \frac{1}{c}(u_{i_j} v - v_{i_j} u)} \left(\frac{1}{c} (u_{i_j} v - v_{i_j} u) \right) = \mathrm{Prim}(u_{i_j} v - v_{i_j} u). \end{aligned}$$

□

Example 7 Consider the list

$$S=[u=6e_1+6e_3+4e_4,\ v=4e_1+3e_2+3e_3]$$

of vectors in a free $\mathbb{Z}$-module $\mathbb{Z}e_1+\cdots+\mathbb{Z}e_4$. By Proposition 2, we obtain

$$\mathrm{Sat}_{\mathbb{Z}}(\langle u,v\rangle_{\mathbb{Z}})=\langle \mathrm{Prim}(u),\,\mathrm{Prim}(6v-4u),\,\mathrm{Prim}(4v-0u)\rangle_{\mathbb{Z}}$$

$$=\langle \mathrm{Prim}(6e_1+6e_3+4e_4),\,\mathrm{Prim}(9e_2-3e_3-8e_4),\,\mathrm{Prim}(4e_1+3e_2+3e_3)\rangle_{\mathbb{Z}}$$

$$=\langle 3e_1+3e_3+2e_4,\,9e_2-3e_3-8e_4,\,4e_1+3e_2+3e_3\rangle_{\mathbb{Z}}.$$

Let $\mathbf{A}$ be a ring, $a\in\mathbf{A}$, and M be a submodule of a free $\mathbf{A}$-module E. Denote by

$$(M:a)=\{u\in E\mid\ a\,u\in M\}$$

a submodule of E containing M.

Proposition 3 *Let $\mathbf{R}$ be a domain with quotient field $\mathbf{K}$, and consider a finite list $S=[s_1,\dots,s_n]$ of nonzero vectors in a free $\mathbf{R}$-module E with basis $(e_i)_{i\in I}$. Let $\mathrm{Echel}(S)=[v_1,\dots,v_r]$ ($r=\dim_{\mathbf{K}}(\mathbf{K}\,s_1+\cdots+\mathbf{K}\,s_n)\le n$) be the list obtained after transforming S into a primitive triangular list over the quotient field $\mathbf{K}$ with Algorithm 2 (E being replaced with the finite-rank free $\mathbf{R}$-module generated by the e_i's on which the s_j's depend). Then*

$$\mathrm{Sat}(\mathbf{R}\,s_1+\cdots+\mathbf{R}\,s_n)=((\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r):\delta^r)=((\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r):\delta^n),$$

where $u_i=(1/\delta_i)w_i$, $w_i\in E$, $\delta_i\in\mathbf{R}\backslash\{0\}$, and $\delta=\mathrm{lcm}(\delta_1,\dots,\delta_r)=\prod_{i=1}^r\delta_i$.

Proof. Let $u\in(\mathbf{K}\,s_1+\cdots+\mathbf{K}\,s_n)\cap E=(\mathbf{K}\,v_1+\cdots+\mathbf{K}\,v_r)\cap E$. There exist $a_1\dots,a_r\in\mathbf{K}$ such that

$$u=a_1v_1+\cdots+a_rv_r.$$

For each $1\le i\le r$, by identifying the $\mathrm{index}(v_i)^{\mathrm{th}}$ coefficient of u, we obtain

$$\begin{cases} a_1\in\mathbf{R},\\ b_{2,1}a_1+a_2\in\mathbf{R},\\ \vdots\\ b_{r,1}a_1+b_{r,2}a_2+\cdots+b_{r,r-1}a_{r-1}+a_r\in\mathbf{R},\end{cases}$$

with $b_{i,j}\in(1/\delta)\mathbf{R}$. It follows that $a_1\in\mathbf{R}$, $a_2\in(1/\delta)\mathbf{R}$, $a_3\in(1/\delta^2)\mathbf{R},\dots,a_r\in(1/\delta^{r-1})\mathbf{R}$, and, thus,

$$u\in(1/\delta^{r-1})(\mathbf{R}\,v_1+\cdots+\mathbf{R}\,v_r)\subseteq(1/\delta^r)(\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r).$$

Hence, $\mathrm{Sat}(\mathbf{R}\,s_1+\cdots+\mathbf{R}\,s_n)=((\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r):\delta^r)$. It remains to note that

$$\begin{aligned}\mathrm{Sat}(\mathbf{R}\,s_1+\cdots+\mathbf{R}\,s_n)&=((\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r):\delta^r)\\&\subseteq((\mathbf{R}\,w_1+\cdots+\mathbf{R}\,w_r):\delta^n)\subseteq\mathrm{Sat}(\mathbf{R}\,s_1+\cdots+\mathbf{R}\,s_n).\end{aligned}$$

□

In the remainder of the paper, the ring $\mathbb{Z}$ can be replaced by any principal ideal domain. The following result is a global version of Theorem 2.

Theorem 4 *Let $S=[s_1,\ldots,s_n]$ be a finite list of nonzero vectors in a free $\mathbb{Z}$-module E with basis $(e_i)_{i\in I}$ and let* $\mathrm{Echel}(S)=[v_1,\ldots,v_r]$ *($r=\dim_{\mathbb{Q}}(\mathbb{Q}\,s_1+\cdots+\mathbb{Q}\,s_n)\le n$) be the list obtained after transforming S into a primitive triangular list over $\mathbb{Q}$ with Algorithm 2 (E being replaced with the finite-rank free $\mathbb{Z}$-module generated by the e_i's on which the s_j's depend). Further, let $u_i=(1/\delta_i)w_i$, where $w_i\in E$, $\delta_i\in\mathbb{Z}\setminus\{0\}$, $\delta=\mathrm{lcm}(\delta_1,\ldots,\delta_r)$, and let $\{p_1,\ldots,p_t\}$ be the set of the prime numbers dividing δ. Then*

$$(1)\qquad\begin{aligned}\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\,s_1+\cdots+\mathbb{Z}\,s_n)&=\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r)\\&=((\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r):\delta^r)=((\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r):\delta^n).\end{aligned}$$

(2) *The following assertions are equivalent:*

(i) $\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r$ *is $\mathbb{Z}$-saturated.*

(ii) *For all $1\le i\le t$, $\mathbb{Z}_{p_i\mathbb{Z}}\,w_1+\cdots+\mathbb{Z}_{p_i\mathbb{Z}}\,w_r$ is $\mathbb{Z}_{p_i\mathbb{Z}}$-saturated.*

(iii) $\dim_{\mathbb{Q}}W=\dim_{\mathbb{F}_{p_1}}W=\cdots=\dim_{\mathbb{F}_{p_t}}W$,
where $W=[w_1,\ldots,w_r]$, $\dim_{\mathbb{Q}}W$ denotes the dimension of $\mathbb{Q}w_1+\cdots+\mathbb{Q}w_r$ as $\mathbb{Q}$-vector space, and $\dim_{\mathbb{F}_{p_i}}W$ denotes the dimension of $\mathbb{F}_{p_i}\bar{w}_1+\cdots+\mathbb{F}_{p_i}\bar{w}_r$ as $\mathbb{F}_{p_i}$-vector space, $\bar{w}_j$ denoting w_j seen in $E\otimes_{\mathbb{Z}}\mathbb{F}_{p_i}$.

(3) *If for $1\le i\le t$, $\{(1/a_{i,1})\epsilon_{i,1},\ldots,(1/a_{i,\ell_i})\epsilon_{i,\ell_i}\}$ is a generating set for $\mathrm{Sat}_{\mathbb{Z}_{p_i\mathbb{Z}}}(\mathbb{Z}_{p_i\mathbb{Z}}\,s_1+\cdots+\mathbb{Z}_{p_i\mathbb{Z}}\,s_n)$ with $\epsilon_{i,j}\in E$ and $a_{i,j}\in\mathbb{Z}\setminus p_i\mathbb{Z}$, then*

$$\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\,s_1+\cdots+\mathbb{Z}\,s_n)=\langle w_1,\ldots,w_r,\epsilon_{1,1},\ldots,\epsilon_{1,\ell_1},\ldots,\epsilon_{t,1},\ldots,\epsilon_{t,\ell_t}\rangle.$$

Proof. (1) This is Proposition 3. The fact that $\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\,s_1+\cdots+\mathbb{Z}\,s_n)=\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r)$ is clear.

(2) The equivalence of (ii) and (iii) follows from Theorem 2.

Let us show that (ii) follows from (i). Let $v=(1/a)u$, $a\in\mathbb{Z}\setminus p_i\mathbb{Z}$ and $u\in E$ be such that $\alpha\,v\in\mathbb{Z}_{p_i\mathbb{Z}}\,w_1+\cdots+\mathbb{Z}_{p_i\mathbb{Z}}\,w_r$ for some $\alpha\in\mathbb{Z}_{p_i\mathbb{Z}}\setminus\{0\}$. It follows that there exists $b\in\mathbb{Z}\setminus\{0\}$ such that $b\,u\in\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r$. But, since $\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r$ is $\mathbb{Z}$-saturated, we infer that $u\in\mathbb{Z}\,w_1+\cdots+\mathbb{Z}\,w_r$, and, thus, $v\in\mathbb{Z}_{p_i\mathbb{Z}}\,w_1+\cdots+\mathbb{Z}_{p_i\mathbb{Z}}\,w_r$.

Now, let us show that (i) follows from (ii). Let $v \in \mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\, w_1 + \cdots + \mathbb{Z}\, w_r)$. By virtue of (1),

$$\delta^r v \in \mathbb{Z}\, w_1 + \cdots + \mathbb{Z}\, w_r. \qquad (0)$$

Further, for all $1 \leq i \leq t$, since $\mathbb{Z}_{p_i\mathbb{Z}}\, w_1 + \cdots + \mathbb{Z}_{p_i\mathbb{Z}}\, w_r$ is $\mathbb{Z}_{p_i\mathbb{Z}}$-saturated, there exists $\alpha_i \in \mathbb{Z} \setminus p_i\mathbb{Z}$ such that

$$\alpha_i v \in \mathbb{Z}\, w_1 + \cdots + \mathbb{Z}\, w_r. \qquad (i)$$

Since $\gcd(\delta^r, \alpha_1, \ldots, \alpha_t) = 1$, there exist $\beta, \beta_1, \ldots, \beta_t \in \mathbb{Z}$ such that $\beta\delta^r + \beta_1\alpha_1 + \cdots + \beta_t\alpha_t = 1$ ($\mathbb{Z}$ being a Bézout domain), and, thus, combining (0), (1),. . .,(t), one gets $v \in \mathbb{Z}\, w_1 + \cdots + \mathbb{Z}\, w_r$, as desired.

(3) We have $\mathrm{Sat}_{\mathbf{A}}(\mathbf{A}\, s_1 + \cdots + \mathbf{A}\, s_n) = \mathrm{Sat}_{\mathbf{A}}(\mathbf{A}\, w_1 + \cdots + \mathbf{A}\, w_r)$ with $\mathbf{A} = \mathbb{Z}$ or $\mathbb{Z}_{p_i\mathbb{Z}}$. It is clear that

$$\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\, s_1 + \cdots + \mathbb{Z}\, s_n) \supseteq \langle w_1, \ldots, w_r, \epsilon_{1,1}, \ldots, \epsilon_{1,\ell_1}, \ldots, \epsilon_{t,1}, \ldots, \epsilon_{t,\ell_t} \rangle =: M.$$

Conversely, let $v \in \mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\, s_1 + \cdots + \mathbb{Z}\, s_n)$. By virtue of (1), we have

$$\delta^r v \in \langle w_1, \ldots, w_r \rangle. \qquad (0)$$

Besides, for all $1 \leq i \leq t$, there exists $\alpha_i \in \mathbb{Z} \setminus p_i\mathbb{Z}$ such that

$$\alpha_i v \in \langle \epsilon_{i,1}, \ldots, \epsilon_{i,\ell_i} \rangle. \qquad (i)$$

Since $\gcd(\delta^r, \alpha_1, \ldots, \alpha_t) = 1$, there exist $\beta, \beta_1, \ldots, \beta_t \in \mathbb{Z}$ such that $\beta\delta^r + \beta_1\alpha_1 + \cdots + \beta_t\alpha_t = 1$, and, thus, combining (0), (1),. . .,(t), one gets $v \in M$, as desired. □

Theorem 4 implies the following algorithm for computing the $\mathbb{Z}$-saturation of a finitely-generated submodule of a free $\mathbb{Z}$-module via prime factorization.

Algorithm 6
Input: A finite list $S = [s_1, \ldots, s_n]$ of nonzero vectors in a free $\mathbb{Z}$-module E with basis $(e_i)_{i \in I}$.
Output: A finite generating set $H \subseteq E$ of $\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\, s_1 + \cdots + \mathbb{Z}\, s_n)$.

1. Compute a finite list $\mathrm{Echel}(S) = [v_1, \ldots, v_r]$ by transforming S into a primitive triangular list over $\mathbb{Q}$ with Algorithm 2 (E being replaced with the finite-rank free $\mathbb{Z}$-module generated by the e_i's on which the s_j's depend). Denote by $v_i = (1/\delta_i)w_i$, where $w_i \in E$, $\delta_i \in \mathbb{Z} \setminus \{0\}$, take $\delta = \mathrm{lcm}(\delta_1, \ldots, \delta_r)$, and compute the set $\{p_1, \ldots, p_t\}$ of the prime numbers dividing δ.

2. For $1 \leq i \leq t$, using Algorithm 2, compute a finite generating set
$$\left\{ \frac{1}{a_{i,1}} \epsilon_{i,1}, \dots, \frac{1}{a_{i,\ell_i}} \epsilon_{i,\ell_i} \right\}$$
for $\mathrm{Sat}_{\mathbb{Z}_{p_i\mathbb{Z}}}(\mathbb{Z}_{p_i\mathbb{Z}}\, s_1 + \cdots + \mathbb{Z}_{p_i\mathbb{Z}}\, s_n)$, with $\epsilon_{i,j} \in E$ and $a_{i,j} \in \mathbb{Z} \setminus p_i\mathbb{Z}$.
3. $H := \{w_1, \dots, w_r, \epsilon_{1,1}, \dots, \epsilon_{1,\ell_1}, \dots, \epsilon_{t,1}, \dots, \epsilon_{t,\ell_t}\}$.

Example 8 (Example 7 revisited) Keeping the notation of Algorithm 6, consider the list

$$S = [s_1 = 6e_1 + 6e_3 + 4e_4,\ s_2 = 4e_1 + 3e_2 + 3e_3]$$

of vectors in a free $\mathbb{Z}$-module $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_4$. Since applying Algorithm 2 we use different rings, we write $\mathrm{Echel}_{\mathbf{R}}(U)$ when we consider the vectors in the list U as elements of $E \otimes_{\mathbb{Z}} \mathbf{R}$. The first call of Algorithm 2 is with $\mathbf{R} = \mathbb{Q}$. We obtain

$$\begin{aligned} \mathrm{Echel}_{\mathbb{Q}}(S) = \left[\frac{1}{4}s_1,\ \frac{1}{3}s_2\right] &= \left[\frac{3}{2}e_1 + \frac{3}{2}e_3 + e_4,\ \frac{4}{3}e_1 + e_2 + e_3\right] \\ &= \left[\frac{1}{2}(3e_1 + 3e_3 + 2e_4),\ \frac{1}{3}(4e_1 + 3e_2 + 3e_3)\right], \end{aligned}$$

$\delta = \mathrm{lcm}(\delta_1, \delta_2) = 2 \vee 3 = 6,\ W = [w_1, w_2] = [3e_1 + 3e_3 + 2e_4,\ 4e_1 + 3e_2 + 3e_3]$,
$$\mathrm{Echel}_{\mathbb{Z}_{2\mathbb{Z}}}(W) = \left[\frac{1}{3}w_1, w_2 - w_1\right],$$
and, hence
$$\mathrm{Sat}_{\mathbb{Z}_{2\mathbb{Z}}}(\mathbb{Z}_{2\mathbb{Z}}\, w_1 + \mathbb{Z}_{2\mathbb{Z}}\, w_2) = \mathbb{Z}_{2\mathbb{Z}}\, w_1 + \mathbb{Z}_{2\mathbb{Z}}\, w_2,$$
and
$$\mathrm{Echel}_{\mathbb{Z}_{3\mathbb{Z}}}(W) = \left[\frac{1}{2}w_1, \frac{1}{4}w_2\right],$$
and, hence,
$$\mathrm{Sat}_{\mathbb{Z}_{3\mathbb{Z}}}(\mathbb{Z}_{3\mathbb{Z}}\, w_1 + \mathbb{Z}_{3\mathbb{Z}}\, w_2) = \mathbb{Z}_{3\mathbb{Z}}\, w_1 + \mathbb{Z}_{3\mathbb{Z}}\, w_2.$$
Therefore,
$$\mathrm{Sat}_{\mathbb{Z}}(\mathbb{Z}\, v_1 + \mathbb{Z}\, v_2) = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2 = \mathbb{Z}\,(3e_1 + 3e_3 + 2e_4) + \mathbb{Z}\,(4e_1 + 3e_2 + 3e_3).$$

The following algorithm is a global version of Algorithm 5. Our goal now is, given a list $[u, s_1, \dots, s_n]$ of vectors in a free $\mathbb{Z}$-module E, to present an algorithm to test whether u is in $\mathrm{Sat}(\langle s_1, \dots, s_n \rangle)$ or not, and, in the case of positive answer, to express u as a linear combination of the generators of $\mathrm{Sat}(\langle s_1, \dots, s_n \rangle)$ computed using Algorithm 6.

Algorithm 7 (Saturation membership test over the integers)

Input: A finite list $[u, s_1, \dots, s_n]$ of vectors in a free $\mathbb{Z}$-module E with basis $(e_i)_{i\in I}$.

Output: An answer to the question whether $u \in \mathrm{Sat}(\langle s_1, \dots, s_n\rangle)$ or not, and, in the case of positive answer, a finite list $[v_1, \dots, v_m]$ of vectors in E generating $\mathrm{Sat}(\langle s_1, \dots, s_n\rangle)$ as a $\mathbb{Z}$-module and a list $[c_1, \dots, c_m]$ of elements in $\mathbb{Z}$ such that $u = c_1v_1 + \cdots + c_mv_m$.

Since the s_j's depend only on a finite number of the e_i's, we can suppose that E has a finite rank.

1. Compute a finite list $\mathrm{Echel}(S) = [v_1, \dots, v_r]$ by transforming S into a primitive triangular list over $\mathbb{Q}$ using Algorithm 2. Denote by $v_i = (1/\delta_i)w_i$, where $w_i \in E$, $\delta_i \in \mathbb{Z} \setminus \{0\}$, take $\delta = \mathrm{lcm}(\delta_1, \dots, \delta_r)$. Test if $u \in \mathbb{Q}w_1 + \ldots + \mathbb{Q}w_r$. If the answer is NO, then return NO. Else, continue. By clearing the denominators, find $\alpha_0 \in \mathbb{Z} \setminus \{0\}$ such that
$$\alpha_0 u \in \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_r \quad (0).$$
Compute the set $\{p_1, \dots, p_t\}$ of the prime numbers dividing δ which is also the set of the prime numbers dividing α_0.

2. For $1 \le i \le t$, using Algorithm 2, compute a finite generating set
$$\left\{\frac{1}{a_{i,1}}\epsilon_{i,1}, \dots, \frac{1}{a_{i,\ell_i}}\epsilon_{i,\ell_i}\right\}$$
for $\mathrm{Sat}_{\mathbb{Z}_{p_i\mathbb{Z}}}(\mathbb{Z}_{p_i\mathbb{Z}}\, s_1 + \cdots + \mathbb{Z}_{p_i\mathbb{Z}}\, s_n)$, with $\epsilon_{i,j} \in E$ and $a_{i,j} \in \mathbb{Z} \setminus p_i\mathbb{Z}$.

3. For $1 \le i \le t$, using Algorithm 7, compute $\alpha_i \in \mathbb{Z} \setminus p_i\mathbb{Z}$ such that $\alpha_i u \in \mathbb{Z}\epsilon_{i,1} + \cdots + \mathbb{Z}\epsilon_{i,\ell_i}$ (i).

4. Since $\gcd(\alpha_0, \alpha_1, \dots, \alpha_t) = 1$, use a Bézout identity between $\alpha_0, \alpha_1, \dots,$ α_t to transform expressions (0), (1), …, (t) into an expression asserting that
$$u \in \langle w_1, \dots, w_r, \epsilon_{1,1}, \dots, \epsilon_{1,\ell_1}, \dots, \epsilon_{t,1}, \dots, \epsilon_{t,\ell_t}\rangle_{\mathbb{Z}} = \mathrm{Sat}(\langle s_1, \dots, s_n\rangle).$$

Now we give a global version of Theorem 2. The set of prime numbers will be denoted by $\mathbf{P}$. If S is a list of vectors in a $\mathbb{Z}$-module and $p \in \mathbf{P}$, we denote by $\dim_{\mathbb{F}_p} S$ the dimension of $\langle S\rangle_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$ as $\mathbb{F}_p$-vector space.

Theorem 5 *Let S be a finite list of vectors in free $\mathbb{Z}$-module E with basis $(e_i)_{i\in I}$. Let $U := \mathrm{Echel}(S) = [u_1, \dots, u_r]$ ($r = \dim_{\mathbb{Q}} S$) be the list obtained after transforming S into a primitive triangular list over $\mathbb{Q}$ using Algorithm 2 (as the s_j's depend only on a finite number of the e_i's, we can suppose that*

E has a finite rank). Further, let $u_j = (1/\delta_j)w_j$, where $w_j \in E$, $\delta_i \in \mathbb{Z} \setminus \{0\}$, $\delta = \operatorname{lcm}(\delta_1, \dots, \delta_r)$, and let $\{p_1, \dots, p_t\}$ be the set of the prime numbers dividing δ (we call them the essential prime numbers of S or of $\langle S \rangle_{\mathbb{Z}}$). Then the following assertions are equivalent:

(i) $\langle S \rangle_{\mathbb{Z}}$ *is $\mathbb{Z}$-saturated.*

(ii) $\dim_{\mathbb{Q}} S = \dim_{\mathbb{F}_{p_1}} S = \cdots = \dim_{\mathbb{F}_{p_t}} S$.

(iii) The map $\operatorname{rk}(S) : \mathbf{P} \to \mathbb{N}$ *defined by* $\operatorname{rk}(S)(q) = \dim_{\mathbb{F}_q} S$, *is constant equal to* $\dim_{\mathbb{Q}} S$.

(iv) The map $\operatorname{rk}(S) : \mathbf{P} \to \mathbb{N}$ *defined by* $\operatorname{rk}(S)(q) = \dim_{\mathbb{F}_q} S$, *is constant.*

Proof. The equivalence of (i) and (ii) is given by Theorem 4. It is clear that (ii) follows from (iii) and (ii) follows from (iv). To see that (ii) implies (iii), note that if p is a prime number which does not divide δ then we have $\dim_{\mathbb{F}_p} S = \dim_{\mathbb{Q}} S$. Finally, to see that (iv) implies (iii), it suffices to consider a prime number which does not divide δ. □

Next we give a global version of Algorithm 4.

Algorithm 8 (Saturation test over $\mathbb{Z}$ and a witness for nonsaturation if so)

Input: A nonempty finite list $S = [s_1, \dots, s_n]$ of nonzero vectors in a free $\mathbb{Z}$-module E.
Output: An answer to the question whether $\langle S \rangle_{\mathbb{Z}}$ is saturated or not, and, in the case of negative answer, a vector $v \in \operatorname{Sat}(\langle S \rangle_{\mathbb{Z}}) \setminus \langle S \rangle_{\mathbb{Z}}$.

1. Let $(e_i)_{i \in I}$ be a basis for E. Using Algorithm 2 over $\mathbb{Q}$ (as the entries of S depend only on a finite number of the e_i's, we can suppose that E has a finite rank), compute the essential prime numbers $p_1, \dots, p_t$ of S.

2. For $1 \leq \ell \leq t$, use Algorithm 4 with $\mathbf{V} = \mathbb{Z}_{p_\ell \mathbb{Z}}$ to test whether $\langle S \rangle_{\mathbb{Z}_{p_\ell \mathbb{Z}}}$ is saturated.

3. If for some $1 \leq \ell \leq t$, $\langle S \rangle_{\mathbb{Z}_{p_\ell \mathbb{Z}}}$ is not saturated with $u = (1/\alpha)v \in \operatorname{Sat}(\langle S \rangle_{\mathbb{Z}_{p_\ell \mathbb{Z}}}) \setminus \langle S \rangle_{\mathbb{Z}_{p_\ell \mathbb{Z}}}$ as witness ($\alpha \in \mathbb{Z} \setminus p_\ell \mathbb{Z}$ and $v \in E$), then $\langle S \rangle_{\mathbb{Z}}$ is not saturated, and $v \in \operatorname{Sat}(\langle S \rangle_{\mathbb{Z}}) \setminus \langle S \rangle_{\mathbb{Z}}$.

4. If for all $1 \leq \ell \leq t$, $\langle S \rangle_{\mathbb{Z}_{p_\ell \mathbb{Z}}}$ is $\mathbb{Z}_{p_\ell \mathbb{Z}}$-saturated, then $\langle S \rangle_{\mathbb{Z}}$ is $\mathbb{Z}$-saturated.

Example 9 Consider the list

$$S=[s_1=3e_1+3e_3+2e_4,\ s_2=4e_1+3e_2+3e_3]$$

of vectors in a free $\mathbb{Z}$-module $E=\mathbb{Z}e_1+\cdots+\mathbb{Z}e_4$. The first call of Algorithm 2 is with $\mathbf{R}=\mathbb{Q}$. We obtain

$$\mathrm{Echel}_{\mathbb{Q}}(S)=\left[\frac{1}{2}s_1,\ \frac{1}{3}s_2\right],$$

$$\mathrm{Echel}_{\mathbb{Z}_{2\mathbb{Z}}}(S)=\left[\frac{1}{3}s_1, s_2-s_1\right],\quad \mathrm{Sat}_{\mathbb{Z}_{2\mathbb{Z}}}(\mathbb{Z}_{2\mathbb{Z}}\,s_1+\mathbb{Z}_{2\mathbb{Z}}\,s_2)=\mathbb{Z}_{2\mathbb{Z}}\,s_1+\mathbb{Z}_{2\mathbb{Z}}\,s_2,$$

and

$$\mathrm{Echel}_{\mathbb{Z}_{3\mathbb{Z}}}(S)=\left[\frac{1}{2}s_1, \frac{1}{4}s_2\right],\quad \mathrm{Sat}_{\mathbb{Z}_{3\mathbb{Z}}}(\mathbb{Z}_{3\mathbb{Z}}\,s_1+\mathbb{Z}_{3\mathbb{Z}}\,s_2)=\mathbb{Z}_{3\mathbb{Z}}\,s_1+\mathbb{Z}_{3\mathbb{Z}}\,s_2.$$

Therefore, $\langle S\rangle_{\mathbb{Z}}$ is $\mathbb{Z}$-saturated ($\dim_{\mathbb{Q}} S=\dim_{\mathbb{F}_2} S=\dim_{\mathbb{F}_3} S=2$).

Example 10 Consider the abelian group

$$G=\langle a,b,c,d\rangle \text{ with } ab^2d^3=e,\ a^3c^4=d,\ a^2bc=e.$$

We want to answer the question whether G is torsion-free or not, and, in the case of negative answer, to give a torsion-element in G ($\neq e$). In terms of $\mathbb{Z}$-modules, considering the list

$$S=[s_1=e_1+2e_2+3e_4,\ s_2=3e_1+4e_3-e_4,\ s_3=2e_1+e_2+e_3]$$

of vectors in a free $\mathbb{Z}$-module $E=\mathbb{Z}e_1+\cdots+\mathbb{Z}e_4$, we want to answer the question whether $\langle S\rangle_{\mathbb{Z}}$ is saturated or not, and, in the case of negative answer, to give a vector $v\in\mathrm{Sat}(\langle S\rangle_{\mathbb{Z}})\setminus\langle S\rangle_{\mathbb{Z}}$.

Executing Algorithm 2 with $\mathbf{V}=\mathbb{Q}$, we obtain

$$\mathrm{Echel}_{\mathbb{Q}}(S)=\left[\frac{1}{3}e_1+\frac{2}{3}e_2+e_4,\ \frac{5}{6}e_1+\frac{1}{6}e_2+e_3,\ \frac{7}{5}e_1+e_2\right],$$

and, thus, $2,3,5$ are the essential prime numbers of S and $\dim_{\mathbb{Q}} S=3$.

Executing Algorithm 4 with $\mathbf{V}=\mathbb{Z}_{2\mathbb{Z}}$, the list S progresses as follows:

$$\begin{aligned}&[e_1+2e_2+3e_4,\ 3e_1+4e_3-e_4,\ 2e_1+e_2+e_3]\\ &\qquad\to\left[\frac{10}{3}e_1+\frac{2}{3}e_2+4e_3,\ 2e_1+e_2+e_3\right]\\ &\qquad\qquad\to\left[-\frac{14}{3}e_1-\frac{10}{3}e_2\right]=\left[-\frac{2}{3}(7e_1+5e_2)\right].\end{aligned}$$

It follows that $\langle S\rangle_{\mathbb{Z}_{2\mathbb{Z}}}$ is not $\mathbb{Z}_{2\mathbb{Z}}$-saturated ($\dim_{\mathbb{F}_2} S=2$) with $-(1/3)(7e_1+5e_2)\in\mathrm{Sat}(\langle S\rangle_{\mathbb{Z}_{2\mathbb{Z}}})\setminus\langle S\rangle_{\mathbb{Z}_{2\mathbb{Z}}}$ as witness, and, thus, $\langle S\rangle_{\mathbb{Z}}$ is not saturated and $7e_1+5e_2\in\mathrm{Sat}(\langle S\rangle_{\mathbb{Z}})\setminus\langle S\rangle_{\mathbb{Z}}$.

Therefore, G is not torsion-free with $x=a^7b^5\neq e$ as a torsion-element.

References

[1] M. Coste, H. Lombardi, and M.-F. Roy, *Dynamical method in algebra: Effective Nullstellensätze.* Annals of Pure and Applied Logic **111** (2001), 203–256.

[2] L. Ducos, C. Quitté, H. Lombardi, and M. Salou, *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* J. Algebra **281** (2004), 604–650.

[3] L. Ducos, S. Monceur, and I. Yengui, *Computing the* $\mathbf{V}$*-saturation of finitely generated submodules of* $\mathbf{V}[X]^m$ *where* $\mathbf{V}$ *is a valuation domain.* J. Symb. Comp. **72** (2016), 196–205.

[4] A. Hadj Kacem and I. Yengui, *Dynamical Gröbner bases over Dedekind rings*, J. Algebra **324** (2010), 12–24.

[5] G. Havas and B.S Majewski, *Extended gcd calculation.* Proceedings of the Twenty-sixth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1995). Congr. Numer. **111** (1995), 104–114.

[6] A.K. Lenstra, H.W. Lenstra Jr, and L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982), 515–534.

[7] I. Yengui, *Dynamical Gröbner bases*, J. Algebra **301** (2006), 447–458.

Faten Ben Amor
Département de Mathématiques,
Faculté des Sciences, Université de Sfax
3000 Sfax, Tunisia.
faten.benamor1@gmail.com

Ihsen Yengui
Département de Mathématiques,
Faculté des Sciences, Université de Sfax
3000 Sfax, Tunisia.
ihsen.yengui@fss.rnu.tn

Please, cite to this paper as published in
Armen. J. Math., V. **13**, N. 1(2021), pp. 1–21