

Smith Normal Form and Integer solutions to linear equations

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
9 November, 2011 (at 23:31)

In this tract, $\text{Gcd}(0, \dots, 0)$ is zero; this, since every integer divides zero.

All matrices (and vectors) are **integer-valued**,^{♥1} unless specified otherwise. So a square matrix \mathbf{R} is **invertible**^{♥1} IFF $\text{Det}(\mathbf{R}) \in \{\pm 1\}$.

For two, say, 3×5 matrices \mathbf{A} and \mathbf{B} , write:

$$\begin{aligned} \mathbf{A} \overset{r}{\sim} \mathbf{B}, & \quad \text{read "A is row equivalent to B";} \\ \mathbf{A} \overset{c}{\sim} \mathbf{B}, & \quad \text{read "A is column equiv. to B";} \\ \mathbf{A} \overset{rc}{\sim} \mathbf{B}, & \quad \text{read "A is rowcol equivalent to B";} \end{aligned}$$

if there exist *invertible* matrices $\overset{3 \times 3}{\mathbf{R}}$ and $\overset{5 \times 5}{\mathbf{C}}$ such that, respectively,

$$\mathbf{RA} = \mathbf{B}; \quad \mathbf{AC} = \mathbf{B}; \quad \mathbf{RAC} = \mathbf{B}.$$

Smith Normal Form

An $\mathbf{r} \times \mathbf{c}$ matrix \mathbf{G}

$$5: \begin{bmatrix} \delta_1 & & & 0 \\ & \delta_2 & & 0 \\ & & \ddots & \vdots \\ & & & \delta_m & 0 \end{bmatrix} \quad \begin{array}{l} \text{(Here, } \mathbf{m} := \text{Min}(\mathbf{r}, \mathbf{c}). \text{ In} \\ \text{this example, } \mathbf{c} \text{ equals } \mathbf{r} + 1. \\ \text{All unshown entries are zero.)} \end{array}$$

is in **Smith form** if its only non-zero entries –the **pivot-values**– are on its main-diagonal. (Zeros are allowed on the main-diagonal). **Smith form** requires that the matrix be integer-valued, and that all non-zero values on the diagonal occur *before* the zeros. Let $\pi = \pi(\mathbf{G})$ denote the number of pivots (non-zero values).

Our $\mathbf{r} \times \mathbf{c}$ matrix \mathbf{G} is in **Smith normal form**

$$6: \begin{bmatrix} \delta_1 & & & & 0 \\ & \ddots & & & \vdots \\ & & \delta_\pi & & \vdots \\ 0 & \dots & \dots & 0 & \dots & 0 \end{bmatrix} \quad \begin{array}{l} \text{(In this example, } \mathbf{m} = \mathbf{r} \\ \text{and } \pi = \mathbf{r} - 1. \text{ Thus } \delta_m \text{ is} \\ \text{necessarily 0.)} \end{array}$$

if, in addition, the pivots-values are positive *and*

$$7: \quad \delta_1 \bullet \dots \bullet \delta_{\pi-1} \bullet \delta_\pi \bullet \dots \bullet \delta_m.$$

(This divisibility-condition forces zeros on the diagonal to occur last.)

^{♥1}More generally, our matrices' entries come from a *euclidean domain, ED*. An *invertible* \mathbf{R} has $\text{Det}(\mathbf{R}) \in \text{Units}(ED)$. For row operations, we may: *Add any ED-multiple of a row to another; Multiply a row by any ED-unit*. Ditto for column-ops.

Elementary row operations. Applied to an $\mathbf{r} \times \mathbf{c}$ matrix Γ , the (elementary) row-operations^{♥1} are

- a: Exchanging two rows.
- b: Adding a \mathbb{Z} -multiple of one row to another.
- c: Multiplying a row by -1 .

Applying a row-op to Γ produces $\mathbf{E}\Gamma$, where \mathbf{E} is an $\mathbf{r} \times \mathbf{r}$ **elementary matrix**. Notice that $\text{Det}(\mathbf{E})$ is ± 1 , since we are allowed to multiply a row only^{♥1} by -1 .

Analogously, there are the **column operations**. Applying a col-op to Γ produces $\Gamma\hat{\mathbf{E}}$, where $\hat{\mathbf{E}}$ is an $\mathbf{c} \times \mathbf{c}$ elementary matrix.

Applying j -many row-ops and k -many col-ops to Γ produces a matrix

$$\mathbf{G} := \mathbf{R}\Gamma\mathbf{C}, \quad \begin{array}{l} \text{where } \mathbf{R} := \mathbf{E}_j \dots \mathbf{E}_2 \mathbf{E}_1 \\ \text{and } \mathbf{C} := \hat{\mathbf{E}}_1 \hat{\mathbf{E}}_2 \dots \hat{\mathbf{E}}_k. \end{array}$$

This \mathbf{R} is an integer matrix with $\text{Det}(\mathbf{R}) \in \{\pm 1\}$. Ditto \mathbf{C} . These are the *bookkeeping* matrices; our \mathbf{R} keeps track of the (cumulative) row-ops, and \mathbf{C} keeps track of the col-ops. Converting Γ to \mathbf{G} via elem. row-ops and col-ops manifests *rowcol-equivalence*.

It turns out that each matrix Γ is rowcol-equivalent to a *unique* Smith-Normal-Form matrix. We write this as $\mathbf{G} := \text{SNF}(\Gamma)$.

8: Smith Normal Form Thm. *Each matrix Γ is rowcol-equiv to some SNF-matrix, \mathbf{G} . Moreover, the SNF is unique. (I.e, no two distinct SNFs are rowcol-equiv.)* \diamond

Existence of SNF. Applying Lemma 10, below, to our $\mathbf{r} \times \mathbf{c}$ matrix Γ , yields an integer α_1 and matrix \mathbf{B} with

$$\dagger: \quad \Gamma \overset{rc}{\sim} \begin{bmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & & & & \\ \vdots & & & & \\ 0 & & & & \mathbf{B} \end{bmatrix}.$$

By induction on the dimensions of a matrix, our

$$\ddagger: \quad \mathbf{B} \overset{rc}{\sim} \begin{bmatrix} \alpha_2 & & & \\ & \ddots & & \\ & & \alpha_m & \end{bmatrix}, \quad \text{where } \mathbf{m} := \text{Min}(\mathbf{r}, \mathbf{c}).$$

Finally, the rowcol equivalence of (\ddagger) can be done *inside* of (\dagger), thanks to the zeros in the first row and first column of $\text{RhS}(\dagger)$. Consequently

$$\Gamma \overset{rc}{\sim} \begin{bmatrix} \alpha_1 & \alpha_2 & & \\ & \ddots & & \\ & & \alpha_m & \end{bmatrix}.$$

Our last obligation to to arrange divisibility. Apply Lemma 9 to the 1:2 submatrix (meaning, the 2×2 matrix formed by rows and columns 1 and 2) of $\begin{bmatrix} \alpha_1 & \cdots & \alpha_m \\ \beta_1 & \cdots & \beta_m \end{bmatrix}$. Now apply Lemma 9 to 1:3, then 1:4, and continue up to the 1: m submatrix. Letting $g := \text{Gcd}(\alpha_1, \dots, \alpha_m)$, we have shown that

$$\Gamma \stackrel{rc}{\sim} \begin{bmatrix} g & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_m \end{bmatrix},$$

where each β number is an integer multiple of g . Now proceed inductively on the β -submatrix. \blacklozenge

9: Lemma. Suppose $\alpha, \beta \in \mathbb{Z}$. Then

$$\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \stackrel{rc}{\sim} \begin{bmatrix} g & 0 \\ 0 & \ell \end{bmatrix},$$

where $g := \text{Gcd}(\alpha, \beta)$ and $\ell := \text{Lcm}(\alpha, \beta)$. \blacklozenge

Proof. Since \mathbb{Z} is a Euclidean domain, there exist integers S, T st. $S\alpha + T\beta = g$. Thus

$$\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \stackrel{c}{\sim} \begin{bmatrix} \alpha & S\alpha \\ 0 & \beta \end{bmatrix} \stackrel{r}{\sim} \begin{bmatrix} \alpha & S\alpha + T\beta \\ 0 & \beta \end{bmatrix} \stackrel{c}{\sim} \begin{bmatrix} g & \alpha \\ 0 & \beta \end{bmatrix}.$$

Take integers J, K with $\alpha = -Jg$ and $\beta = Kg$. Then

$$\begin{bmatrix} g & \alpha \\ \beta & 0 \end{bmatrix} \stackrel{c}{\sim} \begin{bmatrix} g & \alpha + Jg \\ \beta & J\beta \end{bmatrix} = \begin{bmatrix} g & 0 \\ \beta & J\beta \end{bmatrix} \stackrel{r}{\sim} \begin{bmatrix} g & 0 \\ \beta - Kg & J\beta \end{bmatrix} = \begin{bmatrix} g & 0 \\ 0 & JKg \end{bmatrix}.$$

And $JKg = \pm\ell$. So negate column-two if need be. \blacklozenge

10: Lemma. Suppose A is an $\mathbf{r} \times \mathbf{c}$ matrix with $\mathbf{r}, \mathbf{c} \geq 1$. Then

$$A \stackrel{rc}{\sim} \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & B \end{bmatrix}$$

for some integer α and $[\mathbf{r}-1] \times [\mathbf{c}-1]$ matrix B . \blacklozenge

Proof. Write $A = [a_{i,j}]_{i,j}$. Suppose we have a position $\sigma = (i_0, j_0)$ where $a_\sigma \neq 0$. For a different position on the same column, $\tau = (i, j_0)$ with $i \neq i_0$, divide a_σ into a_τ to get a quotient and remainder (integers):

$$a_\sigma = \mathcal{Q} \cdot a_\tau + \mathcal{R}, \quad \text{with } |\mathcal{R}| < |a_\sigma|.$$

Subtracting $\mathcal{Q} \cdot \text{Row}(i_0, A)$ from $\text{Row}(i, A)$ yields a new matrix $A' \stackrel{r}{\sim} A$ with $|a'_\tau| < |a'_\sigma|$.

For each psn $\tau \in \text{ColOrRow}(\sigma)$ with $\tau \neq \sigma$, we can subtract a multiple of σ 's row or column, obtaining a

11: New matrix $A' \stackrel{rc}{\sim} A$ for which $\forall \tau \in \text{ColOrRow}(\sigma)$ with $\tau \neq \sigma$: $|a'_\tau| < |a'_\sigma|$.

Iterating. Let $\text{Min}(A)$ be the minimum of $|a_\sigma|$, taken over all positions σ for which $a_\sigma \neq 0$.

To prove the lemma, WLOG $\text{Min}(A) \neq 0$. Apply the following procedure.

i: Set $\mu := \text{Min}(A)$ and pick σ with $|a_\sigma| = \mu$.

ii: Apply (11) to produce a matrix $A' \stackrel{rc}{\sim} A$ with $0 < \text{Min}(A') \leq \mu$.

iii: If $\text{Min}(A') = \mu$, then **Stop!** Else, set $A := A'$, and go to step (i).

We will eventually **Stop**, since the μ -numbers form a decreasing sequence of posints. When we stop, we have, for the current position σ , that

$$\text{Min}(A') = \text{Min}(A) = |a_\sigma|.$$

But operation (11) forces *all* the other entries in σ 's row and col to have smaller absolute value than a_σ . So the only way that (11) could have *failed* to lower the matrix's $\text{Min}()$, is if

$$\forall \tau \in \text{ColOrRow}(\sigma) \text{ with } \tau \neq \sigma: a'_\tau = 0.$$

And this says that σ is a *pivot-position* for A . Simply swap rows and swap columns so that the pivot is now in position (1, 1). Voila $\text{RhS}(10)$. \blacklozenge

Setting-up uniqueness of SNF. Imagine an $\mathbf{r} \times \mathbf{c}$ matrix A . There are $\binom{\mathbf{r}}{3}$ many ^{♥2} tripletons $\mathcal{R} \subset [1.. \mathbf{r}]$, and $\binom{\mathbf{c}}{3}$ many tripletons $\mathcal{C} \subset [1.. \mathbf{c}]$. Let $A_{\mathcal{R} \times \mathcal{C}}$ denote the induced 3×3 submatrix. Thus

$$\mathcal{S}_3^A := \left\{ \text{Det}(A_{\mathcal{R} \times \mathcal{C}}) \mid \begin{array}{l} \mathcal{R} \subset [1.. \mathbf{r}] \text{ is a tripleton,} \\ \text{and so is } \mathcal{C} \subset [1.. \mathbf{c}] \end{array} \right\}$$

is a set of integers. Our goal is to show that

$$\mathcal{G}_3^A := \text{Gcd}(\mathcal{S}_3^A)$$

is an *invariant* of row-column equivalence.

12: Invariance Lemma. Consider matrices $A \stackrel{rc}{\sim} B$. Then $\mathcal{G}_k^A = \mathcal{G}_k^B$, for each $k = 1, 2, 3, \dots$ \blacklozenge

^{♥2}This $\binom{\mathbf{r}}{3}$ is the *binomial coefficient* “ \mathbf{r} choose 3”. It is the number of ways of choosing 3 objects from \mathbf{r} -many distinct objects. E.g, $\binom{5}{3}$ equals 10.

Pf. WELOG $k = 3$. WELOG, we obtained B from A

by adding $98 \cdot \text{Row}(A, 7)$ to $\text{Row}(A, 5)$.

So ISTShow that $\boxed{\mathcal{G}_3^A \bullet \mathcal{G}_3^B}$; for by symmetry, then, $\mathcal{G}_3^A \bullet \mathcal{G}_3^B$. BTWay, we've done a row-op, so the set \mathcal{C} plays no essential role. Hence, let $A_{\mathcal{R}}$ and $B_{\mathcal{R}}$ mean $A_{\mathcal{R} \times \mathcal{C}}$ and $B_{\mathcal{R} \times \mathcal{C}}$, for some particular choice of \mathcal{C} .

Consider a tripleton $\mathcal{R} \subset [1..r]$. If $\mathcal{R} \not\ni 5$, then $B_{\mathcal{R}} = A_{\mathcal{R}}$.

In contrast, suppose $\boxed{\mathcal{R} \ni 5}$. If $\mathcal{R} \ni 7$, then

$$\text{Det}(B_{\mathcal{R}}) = \text{Det}(A_{\mathcal{R}}).$$

Now suppose $\mathcal{R} \not\ni 7$. Writing \mathcal{R} as $\{5, i, i'\}$, then,

$$\text{Det}(B_{\mathcal{R}}) = \text{Det}(A_{\mathcal{R}}) + 98 \cdot \text{Det}(A_{\{7, i, i'\}}).$$

And \mathcal{G}_3^A divides both $\text{Det}(A_{\mathcal{R}})$ and $\text{Det}(A_{\{7, i, i'\}})$.

In all three cases, we have that $\mathcal{G}_3^A \bullet \text{Det}(B_{\mathcal{R}})$. \blacklozenge

13: Coro.: Uniqueness of SNF. For an $r \times c$ matrix A , let $\mathbf{m} := \text{Min}(r, c)$. Let \mathbf{G} be some SNF of A , as in (6). And let $\pi := \text{Rank}(A)$, i.e, the number of pivots in \mathbf{G} .

Then A has only one SNF, since

For each $k = 1, 2, \dots, \mathbf{m}$:

13†: $\mathcal{G}_k^A \stackrel{\text{note}}{=} \mathcal{G}_k^{\mathbf{G}}$ equals the product $\delta_1 \cdot \delta_2 \cdots \delta_k$.

In particular $\mathcal{G}_1^A \bullet \dots \bullet \mathcal{G}_{\mathbf{m}}^A$. Indeed, the ratios

$$13\ddagger: \frac{\mathcal{G}_2^A}{\mathcal{G}_1^A} \bullet \frac{\mathcal{G}_3^A}{\mathcal{G}_2^A} \bullet \dots \bullet \frac{\mathcal{G}_{\pi}^A}{\mathcal{G}_{\pi-1}^A}. \quad \blacklozenge$$

Pf of (13†). Our \mathbf{G} is as in (6) and (7). To compute, say, $\mathcal{G}_3^{\mathbf{G}}$, take a tripleton $\mathcal{R} = \{i, i', i''\}$ with $i < i' < i''$. For $\text{Det}(\mathbf{G}_{\mathcal{R} \times \mathcal{C}})$ to be non-zero, necessarily $\mathcal{C} = \mathcal{R}$. Thus $\text{Det}(\mathbf{G}_{\mathcal{R} \times \mathcal{C}})$ equals $\delta_i \cdot \delta_{i'} \cdot \delta_{i''}$. Now use (7). \blacklozenge

Pf of uniqueness. Courtesy (13†), sequence $(\mathcal{G}_k^A)_{k=1}^{\mathbf{m}}$ determines the $(\delta_k)_{k=1}^{\mathbf{m}}$ sequence. \blacklozenge

Commentary. Although $\mathbf{G} := \text{SNF}(A)$ is unique, there can be many pairs (\mathbf{R}, \mathbf{C}) such that \mathbf{RAC} equals \mathbf{G} . Extreme cases are $A := \mathbf{I}$, or A is the zero-matrix. \square

A system of linear equations over \mathbb{Z}

(Matrices are required to be integer-valued.) Consider a matrix-equation of the form

$$14: \quad \begin{matrix} r \times c & c \times 1 \\ \Gamma & \cdot \Sigma \end{matrix} = \begin{matrix} r \times 1 \\ \Upsilon \end{matrix}.$$

The **coefficient matrix** is Γ , and Υ is a **target matrix**. We want to describe the set (it will turn out to be a \mathbb{Z} -lattice) of target matrices. And given a target, we seek the set of **solution matrices** Σ for (14).

Here is the logic. There may be many solutions, S , to $\boxed{\Gamma S = \Upsilon}$, one of which is Σ . But this **augmented system**

$$\begin{matrix} \Gamma \cdot S & = & \Upsilon & \text{and} \\ \mathbf{I} \cdot S & = & \Sigma \end{matrix}$$

(where \mathbf{I} represents an identity matrix) has the **unique solution** $S := \Sigma$. We solve for S using row and column operations. We'll then discover "free variables" which allow us to describe *all* solns S to $\Gamma S = \Upsilon$.

Sequences of matrices. Initialize matrices

$$\begin{matrix} r \times r & r \times c & c \times c \\ R_0 := \mathbf{I} & , & G_0 := \Gamma & , & C_0 := \mathbf{I} \\ \text{and column-vectors} & c \times 1 & r \times 1 \\ & S_0 := \Sigma & , & U_0 := \Upsilon \end{matrix}$$

Row&column operations will modify these, always retaining that

$$\begin{matrix} 1_n, 2_n: & G_n S_n = U_n & \text{and} & U_n = R_n \Upsilon. \\ 3_n, 4_n: & C_n S_n = \Sigma & \text{and} & G_n = R_n \Gamma C_n. \end{matrix}$$

The Row&col ops will be effectuated by elementary matrices E with integer entries and $\text{Det}(E)$ in $\{\pm 1\}$, i.e in $\text{Units}(\mathbb{Z})$.

Row operations. A row-op matrix $\overset{r \times r}{E}$ updates the matrix-sequences as follows:

$$\begin{matrix} 1, 2: & \overbrace{EG_n}^{G_{n+1}} S_n = \overbrace{EU_n}^{U_{n+1}} & \text{and} & \overbrace{EU_n}^{U_{n+1}} = \overbrace{ER_n}^{R_{n+1}} \Upsilon. \\ 4: & \text{and} & \overbrace{EG_n}^{G_{n+1}} = \overbrace{ER_n}^{R_{n+1}} \Gamma C_n. \end{matrix}$$

The other matrices retain their value, i.e $C_{n+1} := C_n$.

Column ops. A column-op $\overset{c \times c}{E}$ updates like this:

$$\begin{aligned}
 1: & \quad \underbrace{G_{n+1}}_{G_n} \underbrace{E^{-1}}_{E^{-1}} \underbrace{S_n}_{S_{n+1}} = U_n \quad \text{and} \\
 3, 4: & \quad \underbrace{C_n E E^{-1}}_{C_{n+1}} \underbrace{S_n}_{S_{n+1}} = \Sigma \quad \text{and} \quad \underbrace{G_n E}_{G_{n+1}} = R_n \Gamma \underbrace{C_n E}_{C_{n+1}}.
 \end{aligned}$$

Result. We rowcol-reduce $G_0 = \Gamma$ to a Smith Form. Supposing this happens at $n=57$, I use bold-face letters to denote

$$\begin{aligned}
 \mathbf{R} & := R_{57}, & \mathbf{G} & := G_{57}, & \mathbf{C} & := C_{57} \\
 & & \mathbf{S} & := S_{57}, & \mathbf{U} & := U_{57}.
 \end{aligned}$$

I henceforth use “ ∞ ” to denote this last stage “57”.

Since we preserved $([1, 2, 3, 4]_n)$, we now have

$$\begin{aligned}
 1_\infty, 2_\infty: & \quad \mathbf{GS} = \mathbf{U} \quad \text{and} \quad \mathbf{U} = \mathbf{R}\Upsilon. \\
 3_\infty, 4_\infty: & \quad \mathbf{CS} = \Sigma \quad \text{and} \quad \mathbf{G} = \mathbf{R}\Gamma\mathbf{C}.
 \end{aligned}$$

The improvement over $([1, 2, 3, 4]_0)$ is that, now, the (new) coefficient matrix \mathbf{G} is in Smith-form, e.g (6).

Pivot- and free-columns. Let π be the number of pivots in \mathbf{G} ; note that $\pi = \text{Rank}(\Gamma)$. Use $\varphi := c - \pi$ for the number of *free columns*.

Decompose \mathbf{G} into its lefthand π -many columns, call it $\overset{r \times \pi}{D}$, and its righthand φ -many columns:

$$15: \quad \mathbf{G} = \left[\begin{array}{c|c} \overset{D}{\begin{matrix} \delta_1 & & & \\ & \ddots & & \\ & & \delta_\pi & \\ 0 & \dots & 0 & \end{matrix}} & \overset{\text{All zero}}{\begin{matrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 0 & \dots & 0 \end{matrix}} \end{array} \right]$$

$$16: \quad \mathbf{C} = \left[\begin{array}{c|c} \mathbf{P} & \mathbf{F} \end{array} \right]$$

Split \mathbf{C} into its *pivot part* $\overset{c \times \pi}{P}$, and its *free part* $\overset{c \times \varphi}{F}$.

Divisibility. From $([1, 2]_\infty)$ and (15), an integer column-vector Υ admits a solution Σ **iff** for each $i = 1, 2, \dots, m$: $\text{Row}(i, \mathbf{R}) \cdot \Upsilon$ is divisible by δ_i .

Another way to state this is:

$$17: \quad \begin{aligned}
 \forall i \in [1 .. \pi] : & \quad \text{Row}(i, \mathbf{R}) \cdot \Upsilon \bullet \delta_i, \quad \text{and} \\
 \forall i \in (\pi .. r] : & \quad \text{Row}(i, \mathbf{R}) \cdot \Upsilon = 0.
 \end{aligned}$$

Lattices

These matrices will give us explicit \mathbb{Z} -bases for the target lattice and the nullspace lattice.

18: Nullspace Theorem. *The \mathbb{Z} -lattice of vectors Σ such that $\Gamma\Sigma = \mathbf{0}_{r \times 1}$, is φ -dimensional. And the set of columns of \mathbf{F} is a \mathbb{Z} -basis for the nullspace-lattice. \diamond*

Proof. Set $\Upsilon := \mathbf{0}_{r \times 1}$ in $([1, 2, 3, 4]_\infty)$. Thus $\mathbf{U} = \mathbf{0}_{r \times 1}$. So \mathbf{S} solves (1_∞) exactly when the top π -many entries in \mathbf{S} are zero; the rest can vary freely. The resulting set of products $\Sigma = \mathbf{CS}$ is exactly the set of products

$$\mathbf{F} \cdot \begin{bmatrix} s_{\pi+1} \\ \vdots \\ s_c \end{bmatrix}, \quad \begin{array}{l} \text{as the } \varphi\text{-many entries} \\ s_{\pi+1}, s_{\pi+2}, \dots, s_{c-1}, s_c \\ \text{vary freely.} \end{array}$$

Finally, the \mathbf{F} -columns are linearly-independent, since those of \mathbf{C} are, since those of \mathbf{C}_0 were. \blacklozenge

A \mathbb{Z} -basis for the set of targets. (Below, use M^t to indicate M -transpose.) We will show that

$$19: \quad \Gamma\mathbf{P} = \mathbf{R}^{-1}\mathbf{D}, \quad \text{i.e.} \quad \overset{r \times r}{\mathbf{R}} \overset{r \times c}{\Gamma} \overset{c \times \pi}{\mathbf{P}} = \overset{r \times \pi}{\mathbf{D}},$$

on our way to establishing our main goal.

20: Target Thm. *The set of Υ for which there exists Σ with $\Gamma\Sigma = \Upsilon$, is a π -dim’al \mathbb{Z} -lattice. A \mathbb{Z} -basis for this lattice is the set of columns of $\Gamma\mathbf{P}$, i.e., of $\mathbf{R}^{-1}\mathbf{D}$. \diamond*

Proof of (20) and (19). Recall that $\Upsilon = \Gamma\Sigma = \Gamma\mathbf{C}\mathbf{S}$. We get *each* target as a product

$$\dagger: \quad \Gamma\mathbf{C} \cdot \left[s_1 \dots s_\pi \ 0 \dots 0 \right]^t,$$

for one particular choice of integer-tuple s_1, \dots, s_π . Why? —because the last φ -many components of \mathbf{S} are mapped by \mathbf{C} , bijectively, to the nullspace of Γ .

Courtesy (16), this set of products (\dagger) is the set

$$\ddagger: \quad \Gamma\mathbf{P} \cdot \left[s_1 \dots s_\pi \right]^t.$$

So we’ve established (20) —*except* that we still need to prove that $\mathbf{R}^{-1}\mathbf{D}$ equals $\Gamma\mathbf{P}$.

Each \mathbf{U} vector arises as a product

$$\mathbf{G} \cdot \left[s_1 \dots s_\pi \ 0 \dots 0 \right]^t,$$

thanks to (1_∞) and (15). And this product equals

$$D \cdot [s_1 \dots s_\pi]^t .$$

Hence $\Upsilon = \mathbf{R}^{-1} \mathbf{U} = \mathbf{R}^{-1} D [s_1 \dots s_\pi]^t$, and this gives the same mapping $(s_1, \dots, s_\pi) \mapsto \Upsilon$ that ΓP does. Consequently, $\mathbf{R}^{-1} D$ minus ΓP is the zero-operator —and so they are equal. ♦

Mapping targets to solns. So the $\mathbf{r} \times \pi$ matrix

$$21: \quad \mathbf{T} := \Gamma P \stackrel{\text{fact}}{=} \mathbf{R}^{-1} D$$

maps “*s-tuples*” $[s_1 \dots s_\pi]^t$ to targets, bijectively, via lefthand multiplication. Thus, in the space of *rational* matrices, our \mathbf{T} has a *lefthand* inverse. ♥³

We pick a particular LH-inverse $\mathbf{D}^\bullet := D^\bullet \cdot \mathbf{R}$ by specifying the following rational lefthand-inverse to D :

$$22: \quad D^\bullet := \begin{bmatrix} 1/\delta_1 & & & 0 \\ & \ddots & & \vdots \\ & & 1/\delta_\pi & 0 \end{bmatrix} \in \text{MAT}_{\pi \times \mathbf{r}}(\mathbb{Q}) .$$

It satisfies ♥⁴ that $D^\bullet D = \mathbf{I}^{\pi \times \pi}$.

In consequence, lefthand-multiplication by *rational* $\mathbf{c} \times \mathbf{r}$ matrix

$$23: \quad \mathbf{M} := P D^\bullet \mathbf{R}$$

carries each target Υ to a particular solution Σ for which $\Gamma \Sigma = \Upsilon$. For each target Υ , then,

$$24: \quad \left\{ \Sigma \mid \Gamma \Sigma = \Upsilon \right\} = M \Upsilon + F \begin{bmatrix} s_{\pi+1} \\ s_{\pi+2} \\ \vdots \\ s_{\mathbf{c}} \end{bmatrix} ,$$

as $s_{\pi+1}, \dots, s_{\mathbf{c}-1}, s_{\mathbf{c}}$ vary over the integers.

We call M our *selector matrix*. It is determined by our particular reduction of Γ to Smith Form.

If we reduced Γ to Smith *Normal* form, then each quotient $\varepsilon_i := \delta_\pi / \delta_i$ is a posint. So

$$M = \frac{1}{\delta_\pi} \cdot \widehat{M}, \quad \text{where the product}$$

$$25: \quad \widehat{M} := P \begin{bmatrix} \varepsilon_1 & & & 0 \dots & 0 \\ & \varepsilon_2 & & 0 \dots & 0 \\ & & \ddots & \vdots & \vdots \\ & & & \varepsilon_\pi & 0 \dots & 0 \end{bmatrix} \mathbf{R}$$

is an *integer* matrix.

Filename: Problems/NumberTheory/snf_lin-eqns.latex

As of: Sunday 01Nov2009. Typeset: 9Nov2011 at 23:31.

♥³Its set of rational LH-inverses is an $[\mathbf{r}-\pi]$ -dimensional “flat”, i.e, an affine subspace.

♥⁴Reverse-product $D D^\bullet$ will not equal $\mathbf{I}^{\mathbf{c} \times \mathbf{c}}$, *unless* $\pi \stackrel{\text{happens}}{=} \mathbf{c}$.