Smith Normal Form and Integer solutions to linear equations

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
27 March, 2024 (at *16:55*)

In this tract, $\mathrm{GCD}(0,\ldots,0)$ 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 $\mathrm{Det}(\mathbf{R}) \in \{\pm 1\}$.

For two, say, 3×5 matrices A and B, write:

$\mathsf{A} \overset{r}{\sim} \mathsf{B}$, read "A is ***row equivalent*** to B";

$\mathsf{A} \overset{c}{\sim} \mathsf{B}$, read "A is ***column equiv.*** to B";

$\mathsf{A} \overset{rc}{\approx} \mathsf{B}$, read "A is ***rowcol equivalent*** to B";

if there exist *invertible* matrices $\overset{3\times3}{\mathbf{R}}$ and $\overset{5\times5}{\mathbf{C}}$ such that, respectively,

$$\mathbf{R}\mathsf{A} = \mathsf{B}; \quad \mathsf{A}\mathbf{C} = \mathsf{B}; \quad \mathbf{R}\mathsf{A}\mathbf{C} = \mathsf{B}.$$

Smith Normal Form

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

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

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 $\mathbb{Z}$-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: $$\begin{bmatrix} \delta_1 & & & & & 0 \\ & \ddots & & & & \vdots \\ & & \delta_\pi & & & \vdots \\ 0 & \ldots & \ldots & 0 & \ldots & 0 \end{bmatrix}$$ (In this example, $\mathbf{m} = \mathbf{r}$ and $\pi = \mathbf{r}-1$. Thus $\delta_{\mathbf{m}}$ is necessarily 0.)

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

7: $$\delta_1 \bullet\!| \ldots \bullet\!| \delta_{\pi-1} \bullet\!| \delta_\pi \bullet\!| \cdots \bullet\!| \delta_{\mathbf{m}}.$$

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

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 $\mathsf{E}\Gamma$, where E is an $\mathbf{r}\times\mathbf{r}$ ***elementary matrix***. Notice that $\mathrm{Det}(\mathsf{E})$ 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 $\Gamma\widehat{\mathsf{E}}$, where $\widehat{\mathsf{E}}$ is an $\mathbf{c}\times\mathbf{c}$ elementary matrix.

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

$$\mathbf{G} := \mathbf{R}\Gamma\mathbf{C}, \quad \text{where } \mathbf{R} := \mathsf{E}_j\cdots\mathsf{E}_2\mathsf{E}_1 \text{ and } \mathbf{C} := \widehat{\mathsf{E}}_1\widehat{\mathsf{E}}_2\cdots\widehat{\mathsf{E}}_k.$$

This $\mathbf{R}$ is an integer matrix with $\mathrm{Det}(\mathbf{R}) \in \{\pm1\}$. 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 $\mathbf{G} := \mathit{SNF}(\Gamma)$.

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.)* ◊

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

†: $$\Gamma \overset{rc}{\approx} \begin{bmatrix} \alpha_1 & 0\ 0 \cdots 0 \\ 0 & \\ \vdots & \mathsf{B} \\ 0 & \end{bmatrix}.$$

By induction on the dimensions of a matrix, our

‡: $$\mathsf{B} \overset{rc}{\approx} \begin{bmatrix} \alpha_2 & & \\ & \ddots & \\ & & \alpha_{\mathbf{m}} \end{bmatrix}, \quad \text{where } \mathbf{m} := \mathrm{Min}(\mathbf{r},\mathbf{c}).$$

Finally, the rowcol equivalence of (‡) can be done *inside* of (†), thanks to the zeros in the first row and first column of RhS(†). Consequently

$$\Gamma \overset{rc}{\approx} \begin{bmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_{\mathbf{m}} \end{bmatrix}.$$

[♡1] More generally, our matrices' entries come from a *euclidean domain*, *ED*. An *invertible* $\mathbf{R}$ has $\mathrm{Det}(\mathbf{R}) \in \mathrm{Units}(\mathit{ED})$. 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.

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 $\begin{bmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_{\mathbf{m}} \end{bmatrix}$. Now apply Lemma 9 to 1:3, then 1:4, and continue up to the 1:$\mathbf{m}$ submatrix. Letting $g := \mathrm{GCD}(\alpha_1, \ldots, \alpha_{\mathbf{m}})$, we have shown that

$$\Gamma \overset{rc}{\approx} \begin{bmatrix} g & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_{\mathbf{m}} \end{bmatrix},$$

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

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

$$\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \overset{rc}{\approx} \begin{bmatrix} g & 0 \\ 0 & \ell \end{bmatrix},$$

where $g := \mathrm{GCD}(\alpha, \beta)$ and $\ell := \mathrm{LCM}(\alpha, \beta)$. ♢

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

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

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

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

And $\text{-}JKg = \frac{\text{-}Jg \cdot Kg}{g} = \frac{\alpha\beta}{g} = \pm\ell$. So negate column-two if need be. ♦

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

$$\mathsf{A} \overset{rc}{\approx} \begin{bmatrix} \alpha & 0 \cdots 0 \\ 0 & \\ \vdots & \mathsf{B} \\ 0 & \end{bmatrix}$$

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

Proof. Write $\mathsf{A} = [a_{\mathrm{i,j}}]_{\mathrm{i,j}}$. Suppose we have a position $\sigma = (\mathrm{i}_0, \mathrm{j}_0)$ where $a_\sigma \neq 0$. For a *different* position on the same column, $\tau = (\mathrm{i}, \mathrm{j}_0)$ with $\mathrm{i} \neq \mathrm{i}_0$, 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 $\mathcal{Q} \cdot \mathrm{Row}(\mathrm{i}_0, \mathsf{A})$ from $\mathrm{Row}(\mathrm{i}, \mathsf{A})$ yields a new matrix $\mathsf{A}' \overset{r}{\sim} \mathsf{A}$ with $|a'_\tau| < |a'_\sigma|$.

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

11: *New matrix* $\mathsf{A}' \overset{rc}{\approx} \mathsf{A}$ *for which* $\forall \tau \in \mathrm{ColOrRow}(\sigma)$ *with* $\tau \neq \sigma$: $|a'_\tau| < |a'_\sigma|$.

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

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

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

ii: Apply (11) to produce a matrix $\mathsf{A}' \overset{rc}{\approx} \mathsf{A}$ with $0 < \mathrm{Min}(\mathsf{A}') \leq \mu$.

iii: If $\mathrm{Min}(\mathsf{A}') = \mu$, then **Stop**! Else, set $\mathsf{A} := \mathsf{A}'$, 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

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

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 Min(), is if

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

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 RhS(10). ♦

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

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

[♡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.

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

$$\mathcal{G}_3^{\mathsf{A}} := \operatorname{GCD}(\mathcal{S}_3^{\mathsf{A}})$$

is an *invariant* of row-column equivalence.

12: Invariance Lemma. *Consider matrices* $\mathsf{A} \overset{rc}{\sim} \mathsf{B}$. *Then* $\mathcal{G}_k^{\mathsf{A}} = \mathcal{G}_k^{\mathsf{B}}$, *for each* $k = 1, 2, 3, \ldots$. ◊

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

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

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

Consider a tripleton $\mathscr{R} \subset [1\,..\,\mathbf{r}]$. If $\mathscr{R} \not\ni 5$, then $\mathsf{B}_{\mathscr{R}} = \mathsf{A}_{\mathscr{R}}$.

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

$$\operatorname{Det}(\mathsf{B}_{\mathscr{R}}) = \operatorname{Det}(\mathsf{A}_{\mathscr{R}}).$$

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

$$\operatorname{Det}(\mathsf{B}_{\mathscr{R}}) = \operatorname{Det}(\mathsf{A}_{\mathscr{R}}) + 98 \cdot \operatorname{Det}(\mathsf{A}_{\{7,\mathsf{i},\mathsf{i}'\}}).$$

And $\mathcal{G}_3^{\mathsf{A}}$ divides both $\operatorname{Det}(\mathsf{A}_{\mathscr{R}})$ and $\operatorname{Det}(\mathsf{A}_{\{7,\mathsf{i},\mathsf{i}'\}})$.

In all three cases, we have that $\mathcal{G}_3^{\mathsf{A}} \bullet\!| \operatorname{Det}(\mathsf{B}_{\mathscr{R}})$. ♦

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

Then A *has only* ***one*** *SNF, since*

13†: *For each* $k = 1, 2, \ldots, \mathbf{m}$:
$\mathcal{G}_k^{\mathsf{A}} \overset{\text{note}}{=\!=} \mathcal{G}_k^{\mathbf{G}}$ *equals the product* $\delta_1 \cdot \delta_2 \cdots \delta_k$.

In particular $\mathcal{G}_1^{\mathsf{A}} \bullet\!| \ldots \bullet\!| \, \mathcal{G}_{\mathbf{m}}^{\mathsf{A}}$. *Indeed, the ratios*

13‡: $$\frac{\mathcal{G}_2^{\mathsf{A}}}{\mathcal{G}_1^{\mathsf{A}}} \bullet\!| \frac{\mathcal{G}_3^{\mathsf{A}}}{\mathcal{G}_2^{\mathsf{A}}} \bullet\!| \ldots \bullet\!| \frac{\mathcal{G}_\pi^{\mathsf{A}}}{\mathcal{G}_{\pi-1}^{\mathsf{A}}}.$$ ◊

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

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

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

A system of linear equations over $\mathbb{Z}$

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

$$14{:}\qquad \overset{\mathbf{r\times c}}{\Gamma}\cdot\overset{\mathbf{c\times 1}}{\Sigma} \;=\; \overset{\mathbf{r\times 1}}{\Upsilon}\,.$$

The ***coefficient matrix*** is Γ, and Υ is $\underline{a}$ ***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 $\boxed{\Gamma\mathsf{S}=\Upsilon}$, one of which is Σ. But this *augmented* system

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

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

Sequences of matrices.

Initialize matrices

$$\mathsf{R}_0 := \overset{\mathbf{r\times r}}{\mathbf{I}}\,,\quad \mathsf{G}_0 := \overset{\mathbf{r\times c}}{\Gamma}\,,\quad \mathsf{C}_0 := \overset{\mathbf{c\times c}}{\mathbf{I}}$$

$$\text{and column-vectors}\quad \mathsf{S}_0 := \overset{\mathbf{c\times 1}}{\Sigma}\,,\quad \mathsf{U}_0 := \overset{\mathbf{r\times 1}}{\Upsilon}\,,$$

Row&column operations will modify these, always retaining that

$$\begin{aligned} &1_n,2_n{:} && \mathsf{G}_n\mathsf{S}_n = \mathsf{U}_n && \text{and} && \mathsf{U}_n = \mathsf{R}_n\Upsilon\,.\\ &3_n,4_n{:} && \mathsf{C}_n\mathsf{S}_n = \Sigma && \text{and} && \mathsf{G}_n = \mathsf{R}_n\Gamma\mathsf{C}_n\,. \end{aligned}$$

The Row&col ops will be effectuated by elementary matrices E with integer entries and $\mathrm{Det}(\mathsf{E})$ in $\{\pm1\}$, i.e in $\mathrm{Units}(\mathbb{Z})$.

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

$$\begin{aligned} &1,2{:} && \overbrace{\mathsf{E}\mathsf{G}_n}^{\mathsf{G}_{n+1}}\mathsf{S}_n = \overbrace{\mathsf{E}\mathsf{U}_n}^{\mathsf{U}_{n+1}} && \text{and} && \overbrace{\mathsf{E}\mathsf{U}_n}^{\mathsf{U}_{n+1}} = \overbrace{\mathsf{E}\mathsf{R}_n}^{\mathsf{R}_{n+1}}\Upsilon\,.\\ &4{:} && && \text{and} && \underbrace{\mathsf{E}\mathsf{G}_n}_{\mathsf{G}_{n+1}} = \underbrace{\mathsf{E}\mathsf{R}_n}_{\mathsf{R}_{n+1}}\Gamma\mathsf{C}_n\,. \end{aligned}$$

The other matrices retain their value, i.e $\mathsf{C}_{n+1}:=\mathsf{C}_n$.

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

$$\begin{aligned} &1{:} && \overbrace{\mathsf{G}_n\mathsf{E}}^{\mathsf{G}_{n+1}}\overbrace{\mathsf{E}^{-1}\mathsf{S}_n}^{\mathsf{S}_{n+1}} = \mathsf{U}_n && \text{and}\\ &3,4{:} && \underbrace{\mathsf{C}_n\mathsf{E}}_{\mathsf{C}_{n+1}}\underbrace{\mathsf{E}^{-1}\mathsf{S}_n}_{\mathsf{S}_{n+1}} = \Sigma && \text{and} && \underbrace{\mathsf{G}_n\mathsf{E}}_{\mathsf{G}_{n+1}} = \mathsf{R}_n\Gamma\underbrace{\mathsf{C}_n\mathsf{E}}_{\mathsf{C}_{n+1}}\,. \end{aligned}$$

Result. We rowcol-reduce $\mathsf{G}_0{=}\Gamma$ to a Smith Form. Supposing this happens at $n{=}57$, I use boldface letters to denote

$$\begin{aligned} \mathbf{R} &:= \mathsf{R}_{57}\,, & \mathbf{G} &:= \mathsf{G}_{57}\,, & \mathbf{C} &:= \mathsf{C}_{57}\\ & & \mathbf{S} &:= \mathsf{S}_{57}\,, & \mathbf{U} &:= \mathsf{U}_{57}\,. \end{aligned}$$

I henceforth use "∞" to denote this last stage "57".

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

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

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 $\pi=\mathrm{Rank}(\Gamma)$. Use $\varphi:=\mathbf{c}-\pi$ for the number of *free columns.*

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

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

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

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

Divisibility.

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

Another way to state this is:

$$17{:}\qquad \begin{aligned} &\forall\mathsf{i}\in[1\,..\,\pi]: && \mathrm{Row}(\mathsf{i},\mathbf{R})\cdot\Upsilon \;\;|\!\bullet\;\; \delta_\mathsf{i}\,, && \text{and}\\ &\forall\mathsf{i}\in(\pi\,..\,\mathbf{r}]: && \mathrm{Row}(\mathsf{i},\mathbf{R})\cdot\Upsilon \;=\; 0\,. \end{aligned}$$

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 $\Gamma\Sigma = \mathbf{0}_{\mathbf{r}\times 1}$, is φ-dimensional. And the set of columns of F is a $\mathbb{Z}$-basis for the nullspace-lattice.* ◊

Proof. Set $\Upsilon := \mathbf{0}_{\mathbf{r}\times 1}$ in $([1,2,3,4]_\infty)$. Thus $\mathbf{U} = \mathbf{0}_{\mathbf{r}\times 1}$. 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

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

Finally, the F-columns are linearly-independent, since those of $\mathbf{C}$ are, since those of C_0 were. ♦

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

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

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 $\Gamma\mathsf{P}$, i.e, of $\mathbf{R}^{-1}\mathsf{D}$.* ◊

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

†: $$\Gamma\mathbf{C}\cdot\Big[s_1 \ldots s_\pi\ \ 0 \ldots 0\Big]^{\mathsf{t}},$$

for one particular choice of integer-tuple $s_1, \cdots, s_\pi$. 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 (†) is the set

‡: $$\Gamma\mathsf{P}\cdot\Big[s_1\ \ldots\ s_\pi\Big]^{\mathsf{t}}.$$

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

Each $\mathbf{U}$ vector arises as a product

$$\mathbf{G}\cdot\Big[s_1 \ldots s_\pi\ \ 0 \ldots 0\Big]^{\mathsf{t}},$$

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

$$\mathsf{D}\cdot\Big[s_1\ \ldots\ s_\pi\Big]^{\mathsf{t}}.$$

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

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

21: $$\mathsf{T} := \Gamma\,\mathsf{P} \overset{\text{fact}}{=\!=} \mathbf{R}^{-1}\mathsf{D}$$

maps ***"s-tuples"*** $\Big[s_1\ \ldots\ s_\pi\Big]^{\mathsf{t}}$ to targets, bijectively, via lefthand multiplication. Thus, in the space of <u>*rational*</u> matrices, our T has a *lefthand* inverse.♡3

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

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

It satisfies♡4 that $\mathsf{D}^\bullet\,\mathsf{D} = \overset{\pi\times\pi}{\mathbf{I}}$.

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

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

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

24: $$\Big\{\Sigma \,\Big|\, \Gamma\Sigma = \Upsilon\Big\} = \mathsf{M}\Upsilon + \mathsf{F}\begin{bmatrix} s_{\pi+1} \\ s_{\pi+2} \\ \vdots \\ s_{\mathbf{c}} \end{bmatrix},$$

as $s_{\pi+1}, \ldots, s_{\mathbf{c}-1}, s_{\mathbf{c}}$ 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 $\varepsilon_{\mathsf{i}} := \delta_\pi/\delta_{\mathsf{i}}$ is a posint. So

25: $$\mathsf{M} = \frac{1}{\delta_\pi}\cdot\widehat{\mathsf{M}}\,, \quad \text{where the product}$$
$$\widehat{\mathsf{M}} := \mathsf{P}\begin{bmatrix} \varepsilon_1 & & & & 0\ldots & 0 \\ & \varepsilon_2 & & & 0\ldots & 0 \\ & & \ddots & \vdots & & \vdots \\ & & & \varepsilon_\pi & 0\ldots & 0 \end{bmatrix}\mathbf{R}$$

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

♡4 Reverse-product $\mathsf{D}\,\mathsf{D}^\bullet$ will <u>not</u> equal $\overset{\mathbf{c}\times\mathbf{c}}{\mathbf{I}}$, *unless* $\pi \overset{\text{happens}}{=\!=} \mathbf{c}$.

is an *integer* matrix.

Filename: `Problems/NumberTheory/snf_lin-eqns.latex`
As of: *Tuesday 01Feb2022.* Typeset: *27Mar2024* at *16:55.*