More Results on the Bases of $\mathbb{Z}^n$ Lattice

This note shows that several results in the SYNASC 2022 conference paper *On the bases of* $\mathbb{Z}^n$ *lattice* by Mehta and Rajasree [1] are tight in the senses specified below. We use its notation for bases, primitive vectors, and minimum distance vectors (MDVs). All norms are Euclidean. The three observations concern one integer certificate in dimension 20.

Let $e_1, \ldots, e_{20}$ be the coordinate vectors, and let $A = [v_1 \ \cdots \ v_{19}]$, where

$$\begin{aligned}
v_1 &= e_{11} + e_{15} - e_{19}, & v_{11} &= e_8 + e_{10} - e_{20},\\
v_2 &= e_4 + e_{12} + e_{13}, & v_{12} &= e_{10} + e_{17} + e_{18},\\
v_3 &= e_2 - e_4 + e_7, & v_{13} &= e_2 - e_{12} - e_{14},\\
v_4 &= e_5 + e_6 - e_9, & v_{14} &= e_1 + e_6 + e_9,\\
v_5 &= e_5 - e_{14} - e_{18}, & v_{15} &= e_{10} + e_{15} + e_{16},\\
v_6 &= e_7 - e_{12} + e_{20}, & v_{16} &= e_8 + e_{13} + e_{19},\\
v_7 &= e_1 - e_8 - e_{12}, & v_{17} &= e_{11} + e_{14} - e_{15},\\
v_8 &= e_{14} + e_{17} - e_{20}, & v_{18} &= e_{15} - e_{16} + e_{19},\\
v_9 &= e_3 - e_{11} + e_{14}, & v_{19} &= e_5 - e_6 - e_{10},\\
v_{10} &= e_3 + e_8 + e_{11}.
\end{aligned}$$

The following integer vector will serve as a normal to the columns of A:

$$\begin{aligned}
c = \big(&-400, -234, 185, -72, 116, 142, 162, -268, 258, -26,\\
&83, -132, 204, -102, -19, 45, -192, 218, 64, -294\big)^T.
\end{aligned}$$

Direct coordinate multiplication gives $c^T v_i = 0$ for each $1 \le i \le 19$. Also $\det[A\ v_i] = 0$, since its final column repeats column i of A; below we show that $|\det[A\ x]| = |c^T x|$ for every $x \in \mathbb{Z}^{20}$. For example, $c^T v_2 = c_4 + c_{12} + c_{13} = -72 - 132 + 204 = 0$ and $c^T v_3 = c_2 - c_4 + c_7 = -234 + 72 + 162 = 0$. Set

$$b_0 = -e_4 + e_{10} - e_{16}.$$

Then $c^T b_0 = 72 - 26 - 45 = 1$. Hence $c^T [A\ b_0] = e_{20}^T$. In particular, c is primitive; the inverse certificate below will also establish that A has rank 19. The absolute coordinates of c, in increasing order, are

$$19, 26, 45, 64, 72, 83, 102, 116, 132, 142, 162, 185, 192, 204, 218, 234, 258, 268, 294, 400.$$

They are distinct, have minimum 19, and every adjacent gap is at least 7. If $0 < \|x\|_2^2 < 3$ for $x \in \mathbb{Z}^{20}$, then x is either $\pm e_j$ or $\pm e_j \pm e_k$ with $j \ne k$. In the first case $|c^T x| \ge 19$. In the second it is a sum or an absolute difference of two distinct absolute coordinates of c, so $|c^T x| \ge 7$. Thus $|c^T x| > 1$ in either case.

Proposition 1 (A strict completion bound fails)**.** *The* 19 *primitive columns of* A *extend to a basis of* $\mathbb{Z}^{20}$*, and each has norm* $\sqrt{3}$*. Nevertheless every unimodular completion* b *satisfies* $\|b\|_2 \ge \sqrt{3}$*, with equality attained.*

Proof. The preceding calculation gives $\|b_0\|_2^2 = 3$ and $c^T b_0 = 1$. Define the signed maximal-minor vector h by $h_j = (-1)^{j+20} \det(A_{\widehat{j}})$, where $A_{\widehat{j}}$ is obtained from A by deleting row j. Thus c is the explicit normal checked above, whereas h is the cofactor normal that computes determinants; we show below that $h = \pm c$. Laplace expansion along the last column gives $\det[A\ b] = h^T b$ for every $b \in \mathbb{Z}^{20}$. The inverse certificate for $[A\ -b_0]$ below shows that $|\det[A\ b_0]| = 1$. Consequently A has rank 19. Both h and c annihilate its columns, so $h = tc$ for some scalar t. Evaluating at b_0 gives $t = \pm 1$ because $c^T b_0 = 1$ and $h^T b_0 = \det[A\ b_0] = \pm 1$. Therefore $h = \pm c$ and $|\det[A\ b]| = |c^T b|$ for every integer b. Thus b_0 is a unimodular completion. Any other completion has $|c^T b| = 1$, which is impossible when $\|b\|_2^2 < 3$. □

This shows that a strictly shorter completion of an *arbitrary prescribed* extendable set of $n-1$ columns cannot be guaranteed. Theorem 2 of [1], which starts with a single primitive vector and chooses the other columns, has different quantifiers and remains consistent with this example.

Proposition 2 (The AMDV hypothesis alone is insufficient)**.** *The basis $B = [A\ -b_0]$ of $\mathbb{Z}^{20}$ is AMDV, yet none of its columns has norm* 1*.*

Proof. The integer matrix C displayed below satisfies $BC = I_{20}$, so B is unimodular. Every column of B has squared norm 3. The rowwise calculations below show that every entry of C has absolute value at least 5, and that distinct absolute entries in each row differ by at least 2. Replacing column i by $x \in \mathbb{Z}^{20}$ gives a basis exactly when $|(Cx)_i| = 1$. If $\|x\|_2^2 < 3$, then x is a signed coordinate vector or a signed sum of two distinct coordinate vectors. In the first case $|(Cx)_i| \geq 5$; in the second it is either a sum of two absolute entries or their difference, so it cannot equal 1. Therefore each column is an MDV of the span of the others. □

The total-unimodularity assumption in Lemma 10 of [1] is substantive: B is not totally unimodular. For instance, its submatrix in rows $3, 11$ and columns $9, 10$ is

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

with determinant 2. Thus the orthonormal conclusion cannot be drawn from AMDV alone; this does not contradict Lemma 10.

Proposition 3 (Ternary combinations attain a different threshold)**.** *For the columns of either A or B, the minimum nonzero norm of a combination with coefficients in $\{-1, 0, 1\}$ is $\sqrt{3}$. Such combinations can nevertheless have norm* 2*.*

Proof. Every ternary combination of the columns of B satisfies $c^T x \in \{-1, 0, 1\}$, because $c^T v_i = 0$ and $c^T(-b_0) = -1$. The same statement holds for A. The initial calculation therefore excludes every nonzero combination of squared norm 1 or 2. Each column has squared norm 3, so the lower bound is attained. On the other hand, $v_2 + v_3 = e_2 + e_7 + e_{12} + e_{13}$ has norm 2. □

This distinguishes the exact ternary minimum from the norms of other short ternary combinations. In particular, the existence of a norm-2 combination does not supply a strictly shorter completion or an MDV reduction.

Inverse certificate

Write $C = (C_{\mathrm{L}} \mid C_{\mathrm{R}})$, with ten columns per block. Direct integer multiplication of the sparse columns of B by the following blocks gives $BC = I_{20}$:

$$C_{\mathrm{L}} = \begin{pmatrix}
352 & 206 & -163 & 63 & -102 & -125 & -143 & 236 & -227 & 23 \\
-231 & -135 & 107 & -41 & 67 & 82 & 94 & -155 & 149 & -15 \\
169 & 99 & -78 & 30 & -49 & -60 & -68 & 113 & -109 & 11 \\
-106 & -62 & 49 & -19 & 31 & 38 & 43 & -71 & 68 & -7 \\
318 & 186 & -147 & 57 & -92 & -113 & -129 & 213 & -205 & 21 \\
-169 & -99 & 78 & -30 & 49 & 60 & 69 & -113 & 109 & -11 \\
107 & 62 & -49 & 19 & -31 & -38 & -43 & 71 & -69 & 7 \\
-318 & -186 & 147 & -57 & 92 & 113 & 129 & -213 & 205 & -21 \\
273 & 160 & -126 & 49 & -79 & -97 & -111 & 183 & -176 & 18 \\
-273 & -160 & 127 & -49 & 79 & 97 & 111 & -183 & 176 & -18 \\
149 & 87 & -69 & 27 & -43 & -53 & -60 & 100 & -96 & 10 \\
318 & 186 & -147 & 57 & -92 & -113 & -129 & 213 & -205 & 21 \\
-169 & -98 & 78 & -30 & 49 & 60 & 68 & -113 & 109 & -11 \\
-106 & -62 & 49 & -19 & 31 & 38 & 43 & -71 & 69 & -7 \\
-279 & -163 & 129 & -50 & 81 & 99 & 113 & -187 & 180 & -18 \\
231 & 135 & -107 & 41 & -67 & -82 & -94 & 155 & -149 & 15 \\
194 & 114 & -90 & 35 & -56 & -69 & -79 & 130 & -125 & 13 \\
121 & 71 & -56 & 22 & -35 & -43 & -49 & 81 & -78 & 8 \\
-212 & -124 & 98 & -38 & 62 & 75 & 86 & -142 & 137 & -14 \\
400 & 234 & -185 & 72 & -116 & -142 & -162 & 268 & -258 & 26
\end{pmatrix}$$

$$C_{\mathrm{R}} = \begin{pmatrix}
-73 & 116 & -179 & 90 & 17 & -40 & 169 & -192 & -57 & 259 \\
48 & -76 & 118 & -59 & -11 & 26 & -111 & 126 & 37 & -170 \\
-35 & 56 & -86 & 43 & 8 & -19 & 81 & -92 & -27 & 124 \\
22 & -35 & 54 & -27 & -5 & 12 & -51 & 58 & 17 & -78 \\
-66 & 105 & -162 & 81 & 15 & -36 & 153 & -174 & -51 & 234 \\
35 & -56 & 86 & -43 & -8 & 19 & -81 & 92 & 27 & -124 \\
-22 & 35 & -54 & 27 & 5 & -12 & 51 & -58 & -17 & 78 \\
66 & -105 & 162 & -81 & -15 & 36 & -152 & 173 & 51 & -234 \\
-57 & 90 & -139 & 70 & 13 & -31 & 131 & -149 & -44 & 201 \\
57 & -90 & 139 & -70 & -13 & 31 & -131 & 149 & 44 & -201 \\
-31 & 49 & -76 & 38 & 7 & -17 & 71 & -81 & -24 & 109 \\
-66 & 105 & -162 & 81 & 15 & -36 & 153 & -173 & -51 & 234 \\
35 & -56 & 86 & -43 & -8 & 19 & -81 & 92 & 27 & -124 \\
22 & -35 & 54 & -27 & -5 & 12 & -51 & 58 & 17 & -78 \\
58 & -92 & 142 & -71 & -13 & 32 & -134 & 152 & 45 & -205 \\
-48 & 76 & -117 & 59 & 11 & -26 & 111 & -126 & -37 & 170 \\
-40 & 64 & -99 & 50 & 9 & -22 & 93 & -106 & -31 & 143 \\
-25 & 40 & -62 & 31 & 6 & -14 & 58 & -66 & -19 & 89 \\
44 & -70 & 108 & -54 & -10 & 24 & -102 & 116 & 34 & -156 \\
-83 & 132 & -204 & 102 & 19 & -45 & 192 & -218 & -64 & 294
\end{pmatrix}$$

For a row i of C, let $m_i = \min_j |C_{ij}|$ and $g_i = \min_{j<k} \big||C_{ij}| - |C_{ik}|\big|$. Reading the two blocks row by row yields the following exact values; the two halves of each row correspond to indices 1–10 and 11–20, respectively:

i	1	2	3	4	5	6	7	8	9	10
m_i	17	11	8	5	15	8	5	15	13	13
g_i	6	4	3	2	6	3	2	5	5	4

i	11	12	13	14	15	16	17	18	19	20
m_i	7	15	8	5	13	11	9	6	10	19
g_i	2	6	3	2	5	4	3	2	4	7

For example, row 4 has smallest absolute entry 5 and smallest gap 2; its entries -7 and -5 realize the gap. These values make the MDV test in the second proposition explicit for all 20 rows and every signed coordinate pair.

References

[1] Shashank K. Mehta and Mahesh Sreekumar Rajasree. On the bases of $\mathbb{Z}^n$ lattice. In *2022 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 100–107. IEEE, 2022.