The shortest vector problem in 3-D

February 3, 2018

In the first version, we assume that we have vectors $\mathbf{u} = (1, 0, 0)$, $\mathbf{v} = (a, b, 0)$ and $\mathbf{w} = (c, d, e)$ and want to find integers i_*, j_* and k_* (not all 0) to minimize

$$\|i_*\mathbf{u} + j_*\mathbf{v} + k_*\mathbf{w}\|.$$

Write $f(i, j, k)$ for $\|i\mathbf{u} + j\mathbf{v} + k\mathbf{w}\|$. Since $f(i, j, k) \geq |ke|$ and $f(1, 0, 0) = 1$, $|k_*e| \leq 1$, so $k_* \leq \lfloor 1/e \rfloor$. Since $f(i, j, k) = f(-i, -j, -k)$, we may assume that $k_* \geq 0$. So we check each value k from 0 to $\lfloor 1/e \rfloor$.

Let us write j_k for the optimal value of j given k. Since $f(i, j, k) \geq |kd + jb|$, for each fixed value of k, $|kd + j_kb| \leq 1$, so

$$\lceil (1/b)(-1 - kd) \rceil \leq j_k \leq \lfloor (1/b)(1 - kd) \rfloor.$$

Given values for k and j, the optimal value for i is the negative of the nearest integer to $kc + ja$. So the total number of values to check according to this algorithm is

$$\sum_{k=0}^{\lfloor 1/e \rfloor} (\lfloor (1/b)(1 - kd) \rfloor - \lceil (1/b)(-1 - kd) \rceil + 1).$$

At the cost of a messier formula, one could improve the number of j values that need to be checked for each k value, since $f(i, j, k) \geq \sqrt{(kd + jb)^2 + (ke)^2}$, so $|kd + j_kb| \leq \sqrt{1 - (ke)^2}$.

In the general case, we have arbitrary $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{R}^3$. One can convert to the case above by rotation and scaling. Alternately, one can apply Gram-Schmidt to find vectors $\mathbf{v}_1$ and $\mathbf{w}_1$ and scalars a, b and c such that

- $\mathbf{v} = a\mathbf{u} + \mathbf{v}_1$
- $\mathbf{w} = b\mathbf{u} + c\mathbf{v}_1 + \mathbf{w}_1$
- $\mathbf{u}$, $\mathbf{v}_1$ and $\mathbf{w}$ are pairwise orthogonal.

Then one can run a modified version of the argument above with $\mathbf{u}$, $\mathbf{v}_1$ and $\mathbf{w}_1$.

1 The general problem

In the general version, we again assume that we have vectors $\mathbf{u} = (1, 0, 0)$, $\mathbf{v} = (a, b, 0)$ and $\mathbf{w} = (c, d, e)$, and one additional vector $\mathbf{t} = (x, y, z)$ and want to find integers i_*, j_* and k_* (possibly all 0) to minimize

$$\|i_*\mathbf{u} + j_*\mathbf{v} + k_*\mathbf{w} - \mathbf{t}\| .$$

We may assume that $\mathbf{t} = p\mathbf{u} + q\mathbf{v} + r\mathbf{w}$ for some $p, q, r \in [0, 1)$. Write $g(i, j, k)$ for $\|i_*\mathbf{u} + j_*\mathbf{v} + k_*\mathbf{w} - \mathbf{t}\|$. As in the first part, we can find an upper bound for the min by considering any one choice for i, j and k. For instance, we can let D be $\min\{g(i, j, k) : i, j, k \in \{0, 1\}\}$.

Since $g(i, j, k) \geq |ke - z|$, $|k_*e - z| \leq D$, so

$$\lceil (z - D)/e \rceil \leq k_* \leq \lfloor (z + D)/e \rfloor .$$

Again, let us write j_k for the optimal value of j given k. Since

$$g(i, j, k) \geq \sqrt{(jb + kd - y)^2 + (ke - z)^2},$$

$\sqrt{(j_kb + kd - y)^2 + (ke - z)^2} \leq D$, which gives that

$$\lceil (1/b)(y - kd - \sqrt{D^2 - (ke - z)^2}) \rceil \leq j_k \leq \lfloor (1/b)(y - kd + \sqrt{D^2 - (ke - z)^2}) \rfloor .$$

For each given pair of values k, j, the optimal value for i is the negative of the closest integer to $ja + kc - x$.