ERRATA:
A CANONICAL FORM FOR POSITIVE DEFINITE MATRICES

MATHIEU DUTOUR SIKIRIĆ, ANNA HAENSCH, JOHN VOIGHT,
AND WESSEL P.J. VAN WOERDEN

This note gives errata for the article *A canonical form for positive definite matrices* [1].

1. Errata

(1) In (2.2.6), the characteristic vector set of L_2 (having Gram matrix A_2) should be lifted to L using closest vectors with respect to L_1 instead. This is what was implemented in the code.

More precisely, Then (2.2.6) should read

$$\mathcal{V}_{\mathrm{cv}}(A) := B_1\mathcal{V}_{\text{wr-cv}}(A_1) \cup \bigcup_{v\in P_2\mathcal{V}_{\mathrm{cv}}(A_2)} (v - B_1\,\mathrm{CV}(A_1, B_1^{-1}(v - \mathrm{proj}(v)))) \tag{2.2.6}$$

where $B_1^{-1} = (B_1^{\mathsf{T}}B_1)^{-1}B_1^{\mathsf{T}}$ is the pseudo-inverse, a right inverse to B_1. This is the union of the well-rounded characteristic vector set for L_1 together with all vectors in the cosets $u_i + L_1$ with minimal distance to L_1, so is well-defined independent of the choice of lifts u_i.

To prove that this is a characteristic vector set, the argument in Theorem 2.2.7(b) should be replaced with the following.

> We now prove (b), checking the conditions (i) and (ii). For part (i), by construction $B_1\mathcal{V}_{\text{wr-cv}}(A_1)$ spans $L_1 = \ker \mathrm{proj}|_L$ and by induction we have that $\mathcal{V}_{\mathrm{cv}}(A_2)$ spans L_2 so that $\mathrm{span}(\mathcal{V}_{\mathrm{cv}}(A_2)) \subseteq L$ projects onto L_2 via proj, so together they span L. Next we show that (ii) holds. First, the lattice L_1 spanned by minimal vectors is well-defined, independent of $U \in \mathrm{GL}_n(\mathbb{Z})$, and $\mathcal{V}_{\text{wr-cv}}(A_1)$ is a characteristic vector set. Hence too the projection L_2 is independent of U; by induction on the dimension, we know that $\mathcal{V}_{\mathrm{cv}}(A_2)$ is a characteristic vector set, and for each vector, the set of minimal vectors in each coset satisfies the necessary transformation transformation property as in the case of $\mathcal{V}_{\text{wr-cv}}$. So altogether, these form a characteristic vector set.
>
> We also write this out in terms of (convenient) bases. Running the algorithm for A and $A' = U^{\mathsf{T}}AU$ with $U \in \mathrm{GL}_n(\mathbb{Z})$, we may suppose that $v_i' = U^{-1}v_i$ and $w_i' = U^{-1}w_i$ by using the transformation property of $\mathrm{Min}(A)$. Then $A_i' = A_i$ and $B_i' = U^{-1}B_i$ for $i = 1, 2$, and so we may further suppose that $u_i' = U^{-1}u_i$ so $P_2' = U^{-1}P_2$. We conclude by noting that CV also has the compatible transformation property: for all $v' \in P_2'\mathcal{V}_{\mathrm{cv}}(A_2')$, we

have

$$\begin{aligned} v' - B_1' \operatorname{CV}(A_1', (B_1')^{-1}(v' - \operatorname{proj}'(v'))) \\ &= U^{-1}v - U^{-1}B_1 \operatorname{CV}(A_1, B_1^{-1}U(U^{-1}v - U^{-1}\operatorname{proj}(v))) \\ &= U^{-1}v - U^{-1}B_1 \operatorname{CV}(A_1, B_1^{-1}(v - \operatorname{proj}(v))). \end{aligned}$$

References

[1] Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel P.J. van Woerden, *A canonical form for positive definite matrices*, Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), ed. Steven Galbraith, Open Book Series 4, Mathematical Sciences Publishers, Berkeley, 2020, 179–195.

Mathieu Dutour Sikirić, Rudjer Bosković Institute, Bijenicka 54, 10000 Zagreb, Croatia
Email address: `mathieu.dutour@gmail.com`

Anna Haensch, Duquesne University, Department of Mathematics and Computer Science, Pittsburgh, Pennsylvania, USA
Email address: `annahaensch@gmail.com`

John Voight, Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: `jvoight@gmail.com`

Wessel van Woerden, Centrum Wiskunde & Informatica, Science Park 123, 1098 XG Amsterdam, Netherlands
Email address: `wvw@cwi.nl`