Electronic Colloquium on Computational Complexity - Reports Series 1996 - available via:

Comment 01 on ECCC TR96-007

FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Corrected proof of Lemma 4.

Lemma 4. *Assume that $a_1, ..., a_n \in R^n$ are linearly independent vectors, $d_1, ..., d_n \in L(a_1, ..., a_n)$ are also linearly independent and $\|d_i\| \leq M$. Then there is a basis of $L(a_1, ..., a_n)$ consisting of vectors no longer than nM. Moreover if $a_i, d_i \in Z^N$ for $i = 1, ..., n$ then the required basis can be found in time polynomial in $\sum_{i=1}^{n}(size(a_i)+size(d_i))$*

We prove the lemma by induction on n. The $n = 1$ case is trivial. Suppose that our assertion holds for lattices of dimension $n-1$. Let F be the hyperplane generated by $d_1, ..., d_{n-1}$ and let $L' = L(a_1, ..., a_n) \cap F$. L' is an $n-1$-dimensional lattice, that is, it has a basis over the integers, (since it is a subgroup of a free Abelian group). According to our inductive assumption L' has a basis $b_1, ..., b_{n-1}$ with $\max_{i=1}^{n-1} \|b_i\| \neq (n-1)M$. Let $F' \neq F$ be a coset of F with $L(a_1, ..., a_n) \cap F' \neq \emptyset$ so that the distance of F and F' is minimal. Clearly this distance is not greater than the distance of d_n from F and therefore it is not greater than M. Let $u \in L(a_1, ..., a_n) \cap F'$. Let a' be the vector that we get from u by projecting it orthogonally to F. By expressing a' as a linear combination of the vectors $d_1, ..., d_{n-1}$, then rounding off the coefficients to the nearest integer we may write a' in the form of $w + a''$, where $w \in L'$ and $\|a''\| \leq \sum_{i=1}^{n-1} \|d_i\| \leq (n-1)M$. $b_1, ..., b_{n-1}, u - w$ is a basis of $L = L(a_1, ..., a_n)$, since, according to the minimality of the distance of F' from F, $L(b_1, ..., b_{n-1}, u - w)$ contains all cosets of L' in L. Since the distance of F and F' is at most M we have that $\|u - a'\| \leq M$, therefore $\|u - w\| \leq (\|u - a'\|^2 + \|a''\|^2)^{1/2} \leq (1 + (n-1)^2)^{1/2} M < nM$ implies that every element of this basis is of length at most nM. The inequality $\|u - w\| \leq (n^2 - 2n)^{1/2} M < nM$ shows that even if we compute a' only approximately with a precision greater than, say, $\frac{1}{n^2}M$ the vector $u - w \in L$ that we get from this approximate value will be shorter than nM. Q.E.D.

Sketch of an alternative proof. There is another perhaps simpler proof. Namely we may define F as the subspace orthogonal to d_n and project $L(a_1, ..., a_n)$ onto F. The image L' is an $n-1$ dimensional lattice. Applying the inductive hypothesis (the images of $d_1, ..., d_{n-1}$ are linearly independent) we get a basis $b_1, ..., b_{n-1}$ of L'. Each b_i is contained in a coset D_i of the one dimensional subspace D generated by d_n. Let v_i be the closest point of $D_i \cap L(a_1, ..., a_n)$ to b_i. $v_1, ..., v_{n-1}, d_n$ is the required basis.