A CRITERION FOR DETECTING THE SAME LATTICE

ZIHENG HUANG

0. Acknowledgement

I would like to thank John Greenlees for patiently explaining to me the criterion given in this note. This is only my attempt at a write-up. I would also like to thank Tim Günaydin for reading an earlier draft of this note and pointing out a missing step in the proof of proposition 2.1.

1. The criterion

Given two sets of vectors $A, B \subset \mathbb{Z}^m$, we would like to tell if they span the same lattice. In other words, we would like to check whether $\operatorname{Span}_{\mathbb{Z}} A = \operatorname{Span}_{\mathbb{Z}} B$.

For every $u, v \in \mathbb{R}^m$, we write $u \cdot v$ for their dot product. If $S \subset \mathbb{R}^m$, we define

$$u \cdot S = \{u \cdot v : v \in S\}.$$

Here is the criterion.

Proposition 1.1. *Let $A, B \subset \mathbb{Z}^m$. The condition $\operatorname{Span}_{\mathbb{Z}} A = \operatorname{Span}_{\mathbb{Z}} B$ is equivalent to the condition that for every $u \in \mathbb{R}^{1\times m}$, we have $u \cdot A \subset \mathbb{Z}$ if and only if $u \cdot B \subset \mathbb{Z}$.*

Before we give the proof, let us recall some basic linear algebra facts.

2. Some linear algebra facts

It is possible to "represent" vectors in the dual space by dotting with some vector. In the proposition below, the dot product has the obvious meaning.

Proposition 2.1. *Let k be a field and $e_1, \ldots, e_r \in k^m$ be linear independent. Then there are vectors $u_1, \ldots, u_r \in k^m$ such that $u_i \cdot e_j = \delta_{ij}$, where δ_{ij} is the Kronecker delta.*

Proof. Let $V = \operatorname{Span}_k \{e_1, \ldots, e_r\}$. Then $V \cong k^r$ via a k-linear map and $e_1, \ldots, e_r$ correspond to the standard basis of k^r under this isomorphism. We can represent this linear map by an $r \times m$ matrix E. Define for each $i = 1, \ldots, r$ a vector u_i by the ith row of E. They satisfy the requirement of the proposition. □

Proposition 2.1 can be understood as saying that the dot product is a nondegenrate bilinear pairing. Thanks to the pairing given by the dot product, we can make the dual vectors live inside the same space as the vectors we care about.

Proposition 2.2. *Take any field $k \supset \mathbb{Q}$. The linear independence of $v_1, \ldots, v_r \in \mathbb{Z}^m$ over $\mathbb{Z}, \mathbb{Q}$ and k coincide.*

Proof. By clearing denominators we can change a $\mathbb{Q}$-linear dependence relation to a $\mathbb{Z}$-linear dependence relation. Thus, $\mathbb{Z}$-linear independence implies $\mathbb{Q}$-linear independence.

If $v_1, \ldots, v_r$ are linearly independent over $\mathbb{Q}$, we may by proposition 2.1, find vectors $u_1, \ldots, u_r \in \mathbb{Q}^m$ such that $u_i \cdot v_j = \delta_{ij}$. By dotting with $u_1, \ldots, u_r$, we see that $v_1, \ldots, v_r$ are linearly independent over k.

Finally, if $v_1, \ldots, v_r$ are linearly independent over k, they are clearly independent over $\mathbb{Z}$. □

Proposition 2.3. *A subgroup L of $\mathbb{Z}^m$ is isomorphic to $\mathbb{Z}^r$ for some $r \leq m$. More explicitly, this means $L = \operatorname{Span}_{\mathbb{Z}} \{e_1, \ldots, e_r\}$ for some $\mathbb{Z}$-linearly independent $e_1, \ldots, e_r$.*

Proof. We induct on m. When $m = 1$, any nontrivial subgroup of $\mathbb{Z}$ is $n\mathbb{Z}$ for some $n \in \mathbb{Z} \setminus \{0\}$, so the proposition is obvious.

Now we show that the proposition holds for $\mathbb{Z}^{m+1}$ provided it holds for $\mathbb{Z}^m$. Consider a nontrivial subgroup $L \subset \mathbb{Z}^{m+1}$.

We have a projection $\pi : L \to \mathbb{Z}$ onto the last coordinate, defined by $\pi(x_1, \ldots, x_{m+1}) = x_{m+1}$ for each $(x_1, \ldots, x_{m+1}) \in L$. Denote $K = \ker \pi$ and $I = \operatorname{im} \pi$. Then K can be regarded as a subgroup of $\mathbb{Z}^m$ and I a subgroup of $\mathbb{Z}$.

By induction hypothesis, we have $e_1, \ldots, e_r \in \mathbb{Z}^m \times \{0\} \subset \mathbb{Z}^{m+1}$ for some $r \leq m$ forming a basis for K. On the other hand, $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. We pick some $e_{r+1} \in L$ such that $\pi(e_{r+1}) = n$.

We are done if we can show that $e_1, \ldots, e_{r+1}$ forms a $\mathbb{Z}$-basis for L. The $\mathbb{Z}$-linear independence of $e_1, \ldots, e_{r+1}$ follows by applying π to any linear dependence relation and then using the linear independence of $e_1, \ldots, e_r$.

Clearly $\operatorname{Span}_{\mathbb{Z}} \{e_1, \ldots, e_{r+1}\} \subset K$. For the reverse containment, take any $x \in L$. Since $\pi(x) = kn$ for some $k \in \mathbb{Z}$, we have $x - ke_{r+1} \in K$ which finishes the proof. □

3. Proof of the criterion

Proof of 1.1. We first deal with the easy direction. Suppose that $\operatorname{Span}_{\mathbb{Z}} A = \operatorname{Span}_{\mathbb{Z}} B$. We show that $u \cdot A \subset \mathbb{Z}$ implies that $u \cdot B \subset \mathbb{Z}$. Then the opposite implication follows by symmetry.

Fix a vector $u \in \mathbb{R}^m$ such that $u \cdot A \subset \mathbb{Z}$. Now, take some $b \in B$. There are $a_1, \dots, a_r \in A$ and $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ such that $b = \lambda_1 a_1 + \cdots + \lambda_r a_r$. Then $u \cdot b = \lambda_1(u \cdot a_1) + \cdots + \lambda_r(u \cdot a_r) \in \mathbb{Z}$. This finishes the proof of the easy direction.

Assume now for every $u \in \mathbb{R}^m$, we have $u \cdot A \subset \mathbb{Z}$ if and only if $u \cdot B \subset \mathbb{Z}$. Fix an $a \in A$. We would like to show that $a \in \operatorname{Span}_{\mathbb{Z}} B$. Then we have $\operatorname{Span}_{\mathbb{Z}} A = \operatorname{Span}_{\mathbb{Z}} B$ by symmetry.

We choose a $\mathbb{Z}$-basis $e_1, \dots, e_r \in \mathbb{Z}^m$ for $\operatorname{Span}_{\mathbb{Z}} B$ using proposition 2.3. They form a basis for the $\mathbb{R}$-vector space $\operatorname{Span}_{\mathbb{R}} B$. Extend $e_1, \dots, e_r$ to a basis $e_1, \dots, e_m$ of $\mathbb{R}^m$. By proposition 2.1, we have vectors $u_1, \dots, u_m \in \mathbb{R}^m$ such that $u_i \cdot e_j = \delta_{ij}$ for each $i, j = 1, \dots, m$.

For each $b \in B$, there are $\mu_1, \dots, \mu_r \in \mathbb{Z}$ such that $b = \mu_1 e_1 + \cdots + \mu_r e_r$. Therefore, $u_1 \cdot B, \dots, u_r \cdot B \subset \mathbb{Z}$. Moreover, for any $c \in \mathbb{R}$, $(cu_{r+1}) \cdot B = \cdots = (cu_m) \cdot B = \{0\} \subset \mathbb{Z}$.

We may express $a = \lambda_1 e_1 + \cdots + \lambda_m e_m$. If one of $\lambda_1, \dots, \lambda_r$ is not an integer, say λ_1, then $u_1 \cdot a = \lambda_1 \notin \mathbb{Z}$ is a contradiction. This shows $\lambda_1 = \cdots = \lambda_r \in \mathbb{Z}$. If one of $\lambda_{r+1}, \dots, \lambda_m$ is nonzero, say λ_{r+1}, then $(\frac{1}{2\lambda_{r+1}} u_{r+1}) \cdot a = \frac{1}{2} \notin \mathbb{Z}$ is a contradiction. This shows $\lambda_{r+1} = \cdots = \lambda_m = 0$.

We are done because $a \in \operatorname{Span}_{\mathbb{Z}} \{e_1, \dots, e_r\} = \operatorname{Span}_{\mathbb{Z}} B$. □