
On the Uniqueness of the Leech Lattice

ZHE-XIAN WAN

It has been found that there is an error in Venkov's proof of the uniqueness of the Leech lattice. A construction of neighbours of even unimodular lattices is studied and is used to modify Venkov's proof so that the error is corrected.

© 1997 Academic Press Limited

1. Introduction

The Leech lattice was introduced by Leech [4] in 1964 and its uniqueness was proved by Conway [1] in 1969. Then, using a construction of neighbours of unimodular lattices and the fact that there is a unique (up to isomorphism) 24-dimensional even unimodular lattice the roots of which generate the root lattice of type $24A_1$, Venkov [5] gave another proof in 1978. His paper [5] was included as a chapter in Conway and Sloane [2] in 1988 and his proof was reproduced in Ebeling [3] in 1994. However, there is an error in Venkov's proof [5], which will be pointed out explicitly at the end of this paper. Now, properties of a construction of neighbours of even unimodular lattices are exhibited and are used to modify Venkov's proof so that the error is corrected.

2. Construction of Neighbours

Two lattices $L$ and $L'$ in $\mathbb{R}^n$ are called neighbours if their intersection $L \cap L'$ has index 2 in each of them.

**Proposition 1.** Let $L$ be a unimodular lattice. Then:

(a) Let $u \in L$, $u/2 \notin L$ and $u^2/4 \in \mathbb{Z}$. Define $L_u = \{x \in L \mid x \cdot u = 0 \pmod{2}\}$ and $L_u^* = L_u \cup (u/2 + L_u)$. Then $L_u^*$ is also a unimodular lattice, $L \cap L_u^* = L_u$, and $L$ and $L_u^*$ are neighbours.

(b) Any neighbour $L'$ of $L$ arises in the way of (a), i.e. $L' = L_u^*$, where $u \in L$, $u/2 \notin L$ and $u^2/4 \in \mathbb{Z}$, iff $L'$ is integral.

(c) Let $u$, $u' \in L$, $u/2$, $u'/2 \notin L$ and $u^2/4$, $u'^2/4 \in \mathbb{Z}$. If $L'' = L_u^*$, then $L_u = L_{u'}$ and $u/2 = u'/2 \pmod{L_u}$.

**Proof.** (a) This assertion can be found in [2, Chapter 17], but no proof was given there. For completeness, we give a proof of (a).

We assert that $L_u \neq L$. Suppose that $L_u = L$; then $x \cdot u = 0 \pmod{2}$ for all $x \in L$; then $x \cdot (u/2) \in \mathbb{Z}$ for all $x \in L$, which implies $u/2 \in L^*$, where $L^*$ denotes the dual lattice of $L$. Since $L$ is unimodular, $L^* = L$. Then $u/2 \notin L$, which is a contradiction. Define $L_u^* = \{x \in L \mid x \cdot u = 1 \pmod{2}\}$; then $L = L_u \cup L_u^*$ is the coset decomposition of $L$ relative to $L_u$, $[L/L_u] = 2$ and $L_u$ is a lattice in $\mathbb{R}^n$. Clearly, $L'' = L_u \cup (u/2 + L_u)$ is an integral lattice in $\mathbb{R}^n$ containing $L_u$, $[L''/L_u] = 2$ and $L \cap L'' = L_u$. Therefore $L''$ is a unimodular lattice in $\mathbb{R}^n$, and $L$ and $L''$ are neighbours.

(b) The 'only if' part follows from (a). Now we are going to prove the 'if' part. Let $L'$ be an integral lattice and $L$ and $L'$ be neighbours. Let $L_d = L \cap L'$. Then $[L/L_d] = [L'/L_d] = 2$ and $L'$ can be written as $L' = L_d \cup (v + L_d)$, where $v \in L'$ and...
Let \( L \) be an even unimodular lattice. Then:

(a) Let \( u \in L \), \( u/2 \not\equiv L \) and \( u^2/4 \in \mathbb{Z} \). Then \( L^u \) is an even unimodular lattice iff \( u^2/8 \in \mathbb{Z} \).

(b) Let \( u, u' \in L \), \( u/2 \not\equiv L \), \( u^2/8 \in \mathbb{Z} \), and \( u/2 = u'/2 \pmod{L} \). Then \( L^u = L^{u'} \) and \( u/2 = u'/2 \pmod{L} \).

**Proof.** (a) By Proposition 1(a), we know that \( L^u \) is a unimodular lattice. For any \( w \in L_{u'} \), we have \( w \cdot u = 0 \pmod{2} \). Since \( L \) is even and \( L \supseteq L_{u'} \), \( w^2 \in 2\mathbb{Z} \). Therefore \( (u/2 + w)^2 = u^2/4 + w \cdot u + w^2 \in 2\mathbb{Z} \) iff \( u^2/4 \in 2\mathbb{Z} \), i.e., \( u^2/8 \in \mathbb{Z} \).

(b) Clearly, \( u = u' + 2w \), where \( w \in L \). Thus \( x \cdot u = x \cdot u' \pmod{2} \) for all \( x \in L \), which implies that \( L_{u'} = L_{u''} \). From \( u/2 = u'/2 + w \), we deduce that \( u^2/4 = u'^2/4 + u' \cdot w + w^2 \). By hypothesis, \( u^2/4, u'^2/4 \) and \( w^2 \) are all even. It follows that \( u' \cdot w = 0 \pmod{2} \), i.e., \( w \in L_{u''} = L_{u''} \). Then \( u/2 = u'/2 \pmod{L_{u''}} \) and \( u/2 + L_{u''} = u'/2 + L_{u''} \). Therefore \( L^u = L^{u''} \).

**Example 1.** Let \( G \) be the extended binary Golay code, which is a doubly even self-dual binary linear \([24, 12, 8]\)-code. Let

\[
L_G = \left\{ \frac{1}{\sqrt{2}}(c + 2y) \mid c \in G \text{ and } y \in \mathbb{Z}^{24} \right\},
\]

where the \( c \)'s are regarded as 24-dimensional vectors, the components of which are real numbers 0 and 1, not elements from \( \mathbb{F}_2 \). It is known that \( L_G \) is an even unimodular lattice in \( \mathbb{R}^{24} \) the roots (i.e., vectors of square length 2) of which generate the root lattice of type 24A1. Let

\[
\Lambda_{24} = \left\{ \frac{1}{\sqrt{2}}(c + 2y) \mid c \in G, \ y \in \mathbb{Z}^{24}, \text{ and } \sum_{i=1}^{24} y_i = 0 \pmod{2} \right\}
\]

\[
\cup \left\{ \frac{1}{\sqrt{2}} \left( \frac{1}{2} 1^{24} + c + 2z \right) \mid c \in G, \ z \in \mathbb{Z}^{24} \text{ and } \sum_{i=1}^{24} z_i = 1 \pmod{2} \right\},
\]

where \( 1^{24} \) is the 24-dimensional all-1 vector. It is also known that \( \Lambda_{24} \) is the Leech lattice, which is an even unimodular lattice in \( \mathbb{R}^{24} \) without roots. Let \( u = (1/\sqrt{2})(-3, -3, 

constant terms are both equal to 1 and their coefficients of $L_u$ and $L_{u/2}$ are both 0 (mod 2).

Therefore

$$\Lambda_n = (L_{\tilde{g}})^n = (L_{\tilde{g}})_a \cup (u/2 + (L_{\tilde{g}})_a).$$

**Example 2.** Let $L = \mathbb{Z}^4$ and $L' = \frac{1}{2}\mathbb{Z} \times 2\mathbb{Z}$. Then $|L/L \cap L'| = |L'/L \cap L'| = 2$. Clearly, $|L/L \cap L'| = |L'/L \cap L'| = 2$. Hence $L$ and $L'$ are neighbours. Since $L'$ is not an integral lattice, it cannot be expressed as $L'' = L_u \cup (u/2 + L_u)$, where $u \in L, u/2 \not\in L, u^2/4 \in \mathbb{Z}$ and $L_u = \{x \in L \mid x \cdot u = 0 \text{ (mod 2)} \}$.

This example shows that the statement ‘All neighbours of a unimodular lattice arise in the way of (a)’, which was stated in [2, Chapter 17] is not correct.

**Example 3.** In Example 1, let $u' = (1/\sqrt{2})1^{24}$. Then $u' \in L_{\tilde{g}}, u'/2 \not\in L_{\tilde{g}}, u'^2/4 = 3 \in \mathbb{Z}$ and $u'^2/8 \not\in \mathbb{Z}$. By Proposition 2(a), $(L_{\tilde{g}})^n$ is not even. Therefore $(L_{\tilde{g}})^n \neq (L_{\tilde{g}})^n$.

Clearly, $u/2 - u'/2 = (1/\sqrt{2})(-2, 0^{23}) \in L_{\tilde{g}}$.

This example shows that the statement ‘for a unimodular (or an even unimodular) lattice $L$, and for $u, u' \in L, u/2, u'/2 \not\in L$, and $u^2/4, u'^2/4 \in \mathbb{Z}, L'' = L''$ iff $u/2 = u'/2$ (mod $L$), which was stated in [2, Chapter 17] (or [3, Chapter 4] respectively), is not correct.

3. The Uniqueness of the Leech Lattice

**Theorem 3 (Conway).** There is a unique (up to isomorphism) 24-dimensional even unimodular lattice without roots.

**Proof.** First we follow Venkov’s proof. Let $L$ be a 24-dimensional even unimodular lattice without roots and let $\theta_L(z)$ be its theta function. Let $\Lambda_{24}$ be the Leech lattice and let $\theta_{\Lambda_{24}}(z)$ be its theta function. Both $\theta_L(z)$ and $\theta_{\Lambda_{24}}(z)$ are modular forms of weight 12. Expanding both of them into power series in $q$, where $q = e^{2\pi i z}$, their constant terms are both equal to 1 and their coefficients of $q^2$ are both 0. Therefore $\theta_L(z) = \theta_{\Lambda_{24}}(z)$. Since there is a vector in $\Lambda_{24}$, say $(1/\sqrt{2}) (1^6, 0^6, 1^8)$, of square length 8, the coefficient of $q^8$ in $\theta_{\Lambda_{24}}(z)$ is $>0$. So, the coefficient of $q^8$ in $\theta_L(z)$ is $>0$, and, hence, there is a vector $u \in L$ such that $u^2 = 8$. Since $(u/2)^2 = 2$ and $L$ has no roots, $u/2 \not\in L$. By Propostions 1(a) and 2(a), $L'' = L_u \cup (u/2 + L_u)$ is an even unimodular lattice in $\mathbb{R}^{24}$. Since $u/2 \in L''$, $L''$ has roots.
We prove that the two roots in $L^*$ generate a root lattice of type $24A_1$. It is sufficient to show that for any two roots $x$, $y \in L^*$ and $x \neq \pm y$, we have $x \cdot y = 0$. We have $x^2 = y^2 = 2$. Assume that $x \cdot y \neq 0$. Then either $x - y$ or $x + y$ is a root, and both belong to $L_0$. But $L_0$ has no root, since $L_0 \subset L$, a contradiction. Therefore $L^* = L_0$.

Let $e_i = (1/\sqrt{2})e_i$, where $e_i = (0^{i-1}, 1, 0^{24-i})$, $i = 1, \ldots, 24$. Then $e_i \cdot e_j = 0$ for $i \neq j$, $e_i^2 = \frac{1}{2}$, and $e_1, \ldots, e_{24}$ is a basis of $\mathbb{R}^n$. Clearly, $2e_i \in L_0$. Under the isomorphism $L^* = L_0$, assume that $v_i \mapsto 2e_i$, $i = 1, \ldots, 24$. Then $v_1, \ldots, v_{24} \in L^*$ with $v_i \cdot v_j = 0$ for $i \neq j$ and $v_i^2 = 2$, $i = 1, \ldots, 24$, and $v_1, \ldots, v_{24}$ is a basis of $\mathbb{R}^n$.

Now we deviate from Venkov’s proof. Since $L^*$ and $L$ are neighbours, by Propositions 1(b) and 2(a), there is a $v \in L^*$ with $v/2 \not\in L^*$, $v^2/8 \not\in \mathbb{Z}$, such that $L = (L^*)_v = (L^*)_v \cup (v/2 + (L^*)_v)$. Assume that $v = \sum_{i=1}^{24} \frac{1}{2}m_i v_i$, $m_i \in \mathbb{Z}$. Since $L^*$ is integral, $v_i \cdot v \in \mathbb{Z}$ ($i = 1, \ldots, 24$), so $m_i \in \mathbb{Z}$. We assert that all $m_i$ are odd. Suppose that $m_i$ is even for some $i$. Then $v_i \cdot v = m_i = 0$ (mod 2), i.e. $v_i \in (L^*)_v \subset L$, which contradicts the assertion that $L$ has no roots.

For any $i > 1$, we have

$$(v_i + v) \cdot v = m_i + m_i = 0 \pmod{2}.$$ 

It follows that $v_1 + v_1 \in (L^*)_v$.

Clearly,

$$m_i = 4q_i + \eta_i,$$

where $q_i \in \mathbb{Z}$ and $\eta_i = \pm 1$, $i = 2, \ldots, 24$.

Then $v' = v - \sum_{i=1}^{24} q_i (2v_i + 2v)$ is of the form $\frac{1}{2}(n_1 v_1 + \eta_1 v_2 + \ldots + \eta_2 v_{24})$, where $n_1$ is odd. Clearly, $v' \in L^*$, $v'/2 \not\in L^*$, $v'^2/8 \not\in \mathbb{Z}$ and $v'/2 = v/2$ (mod $(L^*)_v$). By Proposition 2(b), $(L^*)_v = (L^*)^{v'}$. Therefore, we can assume that

$$v = \frac{1}{2}(n_1 v_1 + \eta_1 v_2 + \ldots + \eta_2 v_{24}).$$

Similarly, $2v_1 \in (L^*)_v$ and we can assume that $n_1 \in \{\pm 1, \pm 3\}$. If $n_1 = \pm 1$, then $v^2 = 12$, i.e. $v^2/8 \not\in \mathbb{Z}$. Therefore $n_1 = \pm 3$. If $\eta_i < 0$ for some $i$, let $\sigma_i$ be the reflection determined by the root $v_i$. Then

$$\sigma_i(v) = v_i \quad \text{for } j \neq i, \quad \sigma_i(v_i) = -v_i,$$

and

$$\sigma_i(L^*)_v = (L^*)_v.$$ 

Clearly,

$$(L^*)^{(L^*)_v} = (L^*)_v \cup \left( \frac{\sigma_i(v)}{2} + (L^*)_v \right) = (L^*)_v \cup \left( \frac{v}{2} + (L^*)_v \right) = (L^*)_v.$$ 

Hence we can assume that $\eta_i = 1$ for all $i > 1$. Similarly, we can assume that $n_1 = -3$. Therefore we can assume that $v = \frac{1}{2}(-3v_1 + v_2 + \ldots + v_{24})$, which satisfies the condition $v \in L^*$, $v/2 \not\in L^*$ and $v^2/8 \in \mathbb{Z}$. By Example 1, $(L_0)^* = \Lambda_{24}$, where $u = (1/\sqrt{2}) (-3, 1^{23})$; therefore we also have $(L^*)_v = \Lambda_{24}$.

**Remark.** In Venkov’s proof [5], the case $v = \frac{1}{2}(-3v_1 + v_2 + \ldots + v_{24})$ is missing and only the incorrect case $v = \frac{1}{2}(v_1 + v_2 + \ldots + v_{24})$ appears. But $v = \frac{1}{2}(v_1 + v_2 + \ldots + v_{24})$ does not satisfy $v^2/8 \in \mathbb{Z}$. By Proposition 2(a), $(L^*)_v$ is not even, so $(L^*)_v \neq \Lambda_{24}$. 

REFERENCES


Received 10 January 1996 and accepted in revised form 2 April 1996

ZHIXIAN WAN

Institute of Systems Science,
Chinese Academy of Science,
Beijing 100080, China

and

Department of Information Theory,
Lund University,
Box 118, S-221 00
Lund, Sweden