Optional Notes on Euclid's Lemma and Basis Representation Theorem

Alex Glandon

December 2025

1 Lemma for Basis Representation Theorem

$n < B^n$ whenever $B \geq 2$

2 Proof of Lemma

$n < B^n$

Because $2^n \leq B^n$ for any $B \geq 2$ then if we can prove $n < 2^n$ that is sufficient.

For example consider $4 < 2^4$,

We can show that as follows:

$$\underbrace{1+1+1+1}_{\text{n terms}} < \underbrace{2 \cdot 2 \cdot 2 \cdot 2}_{\text{n terms}}$$

$$\underbrace{1+1+1+1}_{\text{n terms}} < \underbrace{\underbrace{\underbrace{\underbrace{1+1}_{2}+1+1}_{2\cdot 2}+1+1}_{2\cdot 2\cdot 2}+1+1+1+1}_{2\cdot 2\cdot 2\cdot 2}$$

Because the expansion $2 \cdot 2 \cdot 2 \cdot 2$ above has 4 vertical levels, we know that there at least 4 ones in the series of additions.

Therefore, $4 < 2^4$ and in general $n < B^n$ if $B \geq 2$ by considering similar expansions of additions of ones.

3 Proof 2 of Lemma

$n = \underbrace{1+1+1+1}_{\text{n terms}} \leq 1 + B + B^2 + \cdots + B^{n-1}$

since $B \geq 2$

$1 + B + B^2 + \cdots + B^{n-1} = \sum_{i=0}^{n-1} B^i = \frac{B^n - 1}{B-1}$

Using the equation for $\sum_{i=0}^{n-1} B^i$ from the induction lecture.

$\frac{B^n-1}{B-1} \leq \frac{B^n-1}{2-1} = B^n - 1$

since $B \geq 2$

$B^n - 1 < B^n$

Therefore, $n < B^n$

(from Andrews)

4 Proof 2 of Basis Representation Theorem

We need to show there is a unique set of numbers $C_1, C_2, \cdots, C_{N-2}, C_{N-1}$ with all $0 \leq C_i < B$ that satisfy $A = C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + C_{N-2} \cdot B + C_{N-1}$

Given any representation $A = C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + C_{N-2} \cdot B + C_{N-1}$, if C_{N-1-M} is the first non zero C_i from the right, then we can rewrite A as $C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + C_{N-1-M} \cdot B^M$

This means that

$$
\begin{aligned}
A-1 = C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + C_{N-1-M} \cdot B^M - 1 = \\
C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + (C_{N-1-M} - 1)B^M + (B^M - 1) = \\
C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + (C_{N-1-M} - 1)B^M + (B^M - B^{M-1}) \\
+ (B^{M-1} - B^{M-2}) \\
\vdots \\
+ (B^2 - B) \\
+ (B - 1) \\
= C_1 \cdot B^N + C_2 \cdot B^{N-1} + \cdots + (C_{N-1-M} - 1)B^M + (B-1) \cdot B^{M-1} \\
+ (B-1) \cdot B^{M-2} \\
\vdots \\
+ (B-1) \cdot B^1 \\
+ (B-1) \cdot B^0
\end{aligned}
$$

Since $0 \leq B - 1 < B$, this means there exists a representation for $A - 1$ with each coefficient greater than or equal to zero and less than B.

We can write the number of representations of a number K in base B as $R_B(K)$

We showed above that for each representation of A, we can derive a new representation of $A - 1$, which means $R_B(A-1) \geq R_B(A)$

This also means that $R_B(A) \geq R_B(A+1)$, as we can use the same idea for each representation of $A + 1$

Then we see
$R_B(1) \geq \ \ldots \ \geq R_B(A-2) \geq R_B(A-1) \geq R_B(A) \geq$
$R_B(A+1) \geq R_B(A+2) \geq \ \ldots$

Using the lemma from the beginning of this lecture, $B^A > A$, when $B \geq 2$ we can continue

$R_B(1) \geq \ \ldots \ \geq R_B(A-2) \geq R_B(A-1) \geq R_B(A) \geq$
$R_B(A+1) \geq R_B(A+2) \geq \ \ldots \ \geq R_B(B^A)$

It is easy to show that B^A has at least one representation

So $R_B(B^A) \geq 1$

$1 \cdot B^A + 0 \cdot B^{A-1} + 0 \cdot B^{A-2} + \cdots + 0 \cdot B^1 + 0$

Then we have
$R_B(1) \geq \ \ldots \ \geq R_B(A-2) \geq R_B(A-1) \geq R_B(A) \geq$
$R_B(A+1) \geq R_B(A+2) \geq \ \ldots \ \geq R_B(B^A) \geq 1$

We also know that $R_B(1) = 1$, since the only representation of 1 is 1, because any higher order terms $C_i \cdot B^{N+1-i}$ would make for a number larger than 1 as $B \geq 2$

Then we have
$1 \geq R_B(1) \geq \ \ldots \ \geq R_B(A-2) \geq R_B(A-1) \geq R_B(A) \geq$
$R_B(A+1) \geq R_B(A+2) \geq \ \ldots \ \geq R_B(B^A) \geq 1$

Since $1 \geq R_B(A)$ and $R_B(A) \geq 1$, we know $R_B(A) = 1$ which means there is a unique representation of A in base B.

(from Andrews)