# On the number of lines of theorems in the formal system MIU

Armando B. Matos

Technical Report Series: DCC-97-9

Departamento de Ciência de Computadores – Faculdade de Ciências &

Laboratório de Inteligência Artificial e Ciência de Computadores

Universidade do Porto

Rua do Campo Alegre, 823 4150 Porto, Portugal

Tel: +351+2+6001672 – Fax: +351+2+6003654

http://www.ncc.up.pt/fcup/DCC/Pubs/treports.html

# On the number of lines of theorems in the formal system MIU

Armando B. Matos

1997

**Abstract**

The MIU formal system, introduced by Hofstadter in [Hof79], is a relatively simple example of a formal axiomatic system where the length of proofs can be studied in some detail. Denote by $l(t)$ and $L(t)$ respectively the largest and smallest number of lines of a minimum proof of a theorem with $t$ symbols. We show that $l(t)$ is $\Omega(\log t)$ and that $L(t)$ is $\Omega(t/\log t)$ and $O(t)$.

## 1 The MIU formal system

Even for propositional calculus not much is known about the relationship between the length of a theorem and the length of a corresponding shortest proof. Most studies (see for instance [Tse68, SR77, PBI93, Ajt94, Bus87, Urq92, Urq87]) have considered only a particular family of theorems (such as the pigeonhole family of tautologies) and a particular set of inference rules (such as resolution or Frege systems), establishing lower or upper bounds on the length of the shortest proofs. The length of a proof can be defined as either the number of lines it has or its total number of symbols.

The MIU formal system, introduced by Hofstadter ([Hof79]), is still simpler than the propositional calculus so that the relationship between the length of a theorem and of its shortest proof can be studied in more detail.

The MIU system system is defined as follows.

1. Alphabet: $\Sigma = \{\texttt{m}, \texttt{i}, \texttt{u}\}$
2. Axiom: `mi`
3. Inference rules
   (a) $x\mathrm{i} \rightarrow x\mathrm{iu}$

(b) m$x \to$ m$xx$

(c) $x$iii$y \to x$u$y$

(d) $x$uu$y \to xy$

**Notation.** "$\vdash x$" means that $x$ is a theorem[1] of MIU. "$y \vdash x$" means that $x$ can be derived from $y$ in 0 or more steps.

**Definition 1** *The* MIU graph $G_{MIU} = (V, E)$ *is a directed graph characterized by the following rules.*

- `mi` $\in V$.
- *If* $t_1 \in V$ *and* $t_2$ *results from* $t_1$ *by the application of an inference rule, then* $t_2 \in V$ *and* $(t_1, t_2) \in E$.

*Clearly* $V$ *is the set of theorems of MIU. In Figure 7 we can see a little bit of the MIU graph.*

Notice that the MIU graph contains cycles, for instance

$$\texttt{mi}, \texttt{mii}, \texttt{miiii}, \texttt{miiiiu}, \texttt{miuu}, \texttt{mi}$$

A *simple proof* of $x$ is a simple path from `mi` to $x$.

In this paper we always assume the following

- The size of a theorem is the number of *symbols* it contains,
- The size of a proof is the number of *lines* it contains.

**[Paper structure]**

# 2 Standard proofs

## 2.1 Definition

In [Mat97] it is proved that $y$ is a theorem of MIU iff

$$y = \texttt{m}x,\ x \in \{\texttt{i}, \texttt{u}\}^\star \text{ and } |x|_i \text{ is not a multiple of } 3$$

where $|x|_i$ denotes the number of `i`'s in $x$. A standard proof of every such `m`$x$ is also given. For convenience Figure 2.1 is taken from [Mat97].

[1] We use "theorem" in lower case for MIU theorems and "Theorem" for the results of this paper.

```
            Let nu be the number of u's in x
            Let ni be the number of i's in x
            c ← 3 × nu + ni
            if c ≡ 2 mod 3 then
                    let n be the minimum odd integer such that 2^n ≥ c
            if c ≡ 1 mod 3 then
                    let n be the minimum even integer such that 2^n ≥ c
            else print("mx is not a theorem"); return
            Comment: w will contain successive proof lines
      (1)   w ← mi
      (2)   Use n times rule 3b to set w = mi^(2^n)
      (3)   Use rule 3c to replace left to right, groups iii by u as necessary
      (4)   Use rules 3a, 3c and 3d to eliminate the excess of i's
                   at the right (whose number is a multiple of 3)
            Comment: The last line is the theorem to prove, w = mx
```

Figure 1: Algorithm which generates the proof in MIU of $\mathtt{m}x$

### 2.2 Standard proofs are not shortest

We give an example of a theorem whose shortest proof is not standard. The theorem is `muuui` and both proofs are shown in Figure 2.2. The standard proof has 14 lines while the shortest proof has 9.

### 2.3 Bounds of standard proofs

In this section we establish upper and lower bounds for the number of lines of standard proofs.

**Theorem 1 (Upper bound of standard proofs)** *The number of lines $l$ of a standard proof of a theorem with $t$ symbols satisfies $l < 13t$.*

**Proof.** We follow the description of standard proofs given in Figure 2.1. Consider the proof of $\mathtt{m}x$ and let $t' = t - 1$ be the number of symbols in $x$. We have $t' = n_i + n_u$ where $n_i$ and $n_u$ denote respectively the number of `i`'s and `u`'s in $x$.

Let $c = 3n_u + n_i$. We have $t' \leq c < 3t'$. The number of steps needed to produce $c$ `i`'s does not exceed[2] $n = \lceil \log c \rceil + 1$ The "+1" takes in account the fact that the parity of $n$ is given by the algorithm (it

[2] In this paper the basis of logarithms is assumed to be 2.

| Standard proof | A shortest proof |
|---|---|
| mi | mi |
| mii | mii |
| miiii | miiii |
| miiiiiiii | miiiiiiii |
| miiiiiiiiiiiiiiii | muiiiii |
| muiiiiiiiiiiiii | muuii |
| muuiiiiiiiiii | muuiiuuii |
| muuuiiiiiii | muuiiii |
| muuuiiiiiiiu | muuui |
| muuuiiiiiuu | |
| muuuiiii | |
| muuuiiiiu | |
| muuuiuu | |
| muuui | |

Figure 2: The standard proof of theorem `muuui` has 14 lines but the shortest proof (in lines) has 9.

depends on $c$). The number of lines satisfies

$$\begin{array}{rll} l \leq & 1 & \text{Line "(1)" in Figure 2.1} \\ & +n & \text{Line "(2)" in Figure 2.1} \\ & +n_u & \text{Line "(3)" in Figure 2.1} \\ & +3((2^n - n_u)/3) & \text{Line "(4)" in Figure 2.1} \end{array}$$

where "/" in the last term represents integer division. From $c < 3t'$ we get $n < \lceil \log(3t') \rceil + 1$ so that

$$2^n < 2 \times 2^{\lceil \log(3t') \rceil} \leq 4 \times 3t' = 12t'$$

Thus the number of lines satisfies

$$l \leq n + 1 + 2^n < n + 1 + 12t' < 12t' + \lceil \log(3t') \rceil + 2$$

Let us now express this result in terms of $t = t' + 1$.

$$l < 12(t - 12) + \lceil \log(3t) \rceil = 12t + \lceil \log(3t) \rceil - 10$$

But it is easy to see that, for all $t \geq 1$, we have $t > \lceil \log(3t) \rceil - 10$ so that we finally get $l < 13t$ ⋄

Note. It is possible to get a factor less than 13 by using a different definition of standard proof where the excess of `i`'s is reduced by groups of 6 (using twice rule 3c and then rule 3d) instead of 3.

**Theorem 2 (Exact lower bound of standard proofs)** *The number of lines $l$ of a standard proof of a theorem with $t$ symbols satisfies $l \geq 1 + \lceil \log(t-1) \rceil$. This value is reached by every theorem in the infinite family* $\mathtt{mi}^{2^n}$ *(with $n \geq 0$)*

**Proof.** Notice that no other rule can increase the number of symbols of a line more than rule 3b does. (the application of another rule can result in an equal increase in only a very particular inference $\mathtt{mi} \vdash \mathtt{miu}$). So, the last line of a proof with $l$ lines can not have more than $1 + 2^n$ symbols. If we start with the axiom and apply $n$ times rule 3b we get theorem $\mathtt{mi}^{2^n}$. $\diamond$

# 3 Bounds for general proofs

We will now study the size of shortest proofs. Notice that there are in general several theorems with the same length $t$. So, we will consider both smallest and longest shortest proofs.

**Notation.** Let $t \in \mathbb{N}$. Denote respectively by $l(t)$ ($L(t)$) the smallest (respectively largest) size of a shortest proof of a theorem having $t$ symbols.

**Example 1** *Consider the theorems with 3 symbols. They are* $\mathtt{mii}$, $\mathtt{miu}$ *and* $\mathtt{mui}$, *with shortest proofs respectively (the rules applied are indicated as subscripts)*

$$\mathtt{mi} \vdash_{3b} \mathtt{mii}$$
$$\mathtt{mi} \vdash_{3a} \mathtt{miu}$$
$$\mathtt{mi} \vdash_{3b} \mathtt{mii} \vdash_{3b} \mathtt{miiii} \vdash_{3b} \mathtt{mui}$$

*Then $l(3) = 2$ and $L(3) = 4$. Notice that in general there are proofs (even simple proofs) with an arbitrarily large number of lines.*

As a consequence of the results of the previous section we have.

**Theorem 3 (Some general bounds)** *For every $t \geq 2$*

$$1 + \log(t-1) \leq l(t) \leq L(t) < 13t$$

## 3.1 A lower bound for general proofs

We will now see that, for every $t$, there is some theorem with size $t$ having a shortest proof with at least $k(t/\log t)$ lines where $k$ is some positive fixed constant. In other words, $L(t)$ is $\Omega(t/\log t)$. This result (Theorem 4) is based on two observations: (i) there are in general many (about $2^t/3$) theorems with $t$ symbols and (ii) at each step, the number of possible applications of an inference rule is finite and can be appropriately bounded. So, to prove all those theorems, some of the proofs must have a relatively large number of lines. We begin with two lemmas.

**Lemma 1** *Consider the proof of a theorem having $t$ symbols. If the size of the longest line has $T$ symbols, the proof must have at least $\lceil (T-t)/2 \rceil + 1$ lines.*

**Proof.** Rules 3c and 3d decrease the number of symbols by 2 while rules 3a and 3b increase that number. Then, starting with the $T$ symbol line, we need at least $(T-t)/2$ proof steps to get the theorem; the corresponding number of lines is the number of steps plus 1. $\diamond$

**Lemma 2** *The number of symbols $T$ of the longest line of a minimum proof of a theorem with $t$ symbols satisfies $T \leq 27t$.*

**Proof.** Combining the previous Lemma with Theorem 1 we have

$$(T-t)/2 + 1 \leq l \leq 13t$$

Then $T \leq 27t - 2 < 27t$. $\diamond$

Notice that, as mentioned before, a factor less than 27 can be obtained if an alternative definition of "standard proof" is used.

**Theorem 4** *Consider the proofs of all theorems with size $t \geq 3$. At least one of them has a number of lines $L$ satisfying*

$$L \geq 1 + \left\lceil \frac{t - \log 3}{1 + \log(27t)} \right\rceil$$

**Proof.** The number of theorems with size $t$ is at least $2\lfloor 2^{t-1}/3 \rfloor$. This can be shown by noticing two things. First, every such theorem has the form $\mathtt{m}x$ where $|x| = t - 1$. And, second, for $r = 0$, 1 or 2, the number of sequences with length $t-1$ such that each symbol has 2 possibilities, `i` and `u`, and the number of `i`'s is congruent with $r \pmod 3$, is either $\lfloor 2^{t-1}/3 \rfloor$ or $\lceil 2^{t-1}/3 \rceil$ (see for instance [GKP94], exercise 5.75).

Consider now all proofs of theorems with $t$ symbols such that the longest line has no more than $T$ symbols. At each step, we can apply rules 3a (1 possibility), 3b (1 possibility), 3c (at most $T-3$ possibilities; notice that $T \geq t \geq 3$) and 3d (at most $T-2$ possibilities). It follows that, at each step, there at no more than $2T-3$ applications of an inference rule. The largest number $L$ of lines in such a proof (recall that the first line is always, `mi`) must then satisfy (if $T \geq 3$)

$$(2T-3)^{L-1} \geq 2\lfloor 2^{t-1}/3 \rfloor$$

It follows that, as $T \geq 3$ and $L \geq 2$, we have $(2T)^{L-1} \geq 2^t/3$. Taking the logarithm of both members and using the previous Lemma we get

$$L \geq 1 + \frac{t - \log 3}{1 + \log T} \geq 1 + \frac{t - \log 3}{1 + \log(27t)}$$

$\diamond$

Theorem 4 shows that

$$L(t) \text{ is } \Omega(t/\log(t))$$

This means that, no matter what proofs we consider, there are always proofs requiring a number of lines which is "almost linear" in the length of the theorem.

# 4 Smallest theorems and proofs

The following results were obtained with the help of a Prolog program that builds a database of theorems and corresponding shortest proofs up to a certain number $l$ of lines; we have used $l = 9$ which corresponds to a database containing 15 885 theorems. Then, given a theorem candidate, the program may be instructed to search for the corresponding shortest proofs whose "path" (if the shortest proof has more than $l$ lines) consists of two parts: a sequence of steps up to a theorem $x$ in the database (with a $l$ line shortest proof) and an already computed proof of $x$.

1. In Figure 4 we can see what theorems can be proved with no more than 3 lines.

2. Figure 3 shows the number of theorems with shortest proofs not exceeding $l$ lines, for $l = 1$, 2, ..., 9. Some of these theorems are small while others are very large; for instance, the shortest proof of the following theorem has only 9 lines.

$$\texttt{m}\ \overbrace{\texttt{i}\,\texttt{i}\cdots\texttt{i}}^{256\ \texttt{i's}}$$

3. Figure 5 shows bounds (see Theorems 1 and 2) and exact values of $l(t)$ and $L(t)$ for small values of $t$ (see the definitions at the beginning of Section 3).

4. Finally in Figure 6 we compare the lower and upper bounds of $L(t)$ for a few values of $t$.

# 5 Conclusions

We have establish that a shortest proof of a theorem having $t$ symbols has at least $O(\log(t))$ and at most $O(t)$ lines and that the lower bound is exact for a family of theorems. In [Ant97] a different class of proofs is considered from which a bound of $O(max\{n_u, \log(t)\})$ results. We have also shown that the largest number of lines of a shortest proof of such a theorem is $\Omega(t/\log t)$. The proof is based on an counting argument (Information theory) and it is not constructive. It would be interesting to exhibit an explicit family of theorems requiring proofs with this number of lines. It is not even known if this bound is exact; could it be $\Omega(t)$?

| Number of lines up to | Number of theorems |
|---|---|
| 1 | 1 |
| 2 | 3 |
| 3 | 6 |
| 4 | 11 |
| 5 | 25 |
| 6 | 69 |
| 7 | 282 |
| 8 | 1730 |
| 9 | 15885 |

Figure 3: Number of theorems with shortest proofs not exceeding 9 lines

| Theorem | Proof | Number of lines |
|---|---|---|
| `mi` | `mi` | 1 |
| `mii` | `mi, mii` | 2 |
| `miu` | `mi, miu` | 2 |
| `miiii` | `mi, mii, miiii` | 3 |
| `miiu` | `mi, mii, miiu` | 3 |
| `miuiu` | `mi, miu, miuiu` | 3 |

Figure 4: Theorems with proofs not exceeding 3 lines

| $t$ | Lower bound | $l(t)$ | Standard | $L(t)$ | Standard | Upper bound |
|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 1 | 26 |
| 3 | 2 | 2 | 2 | 4 | 4 | 39 |
| 4 | 3 | 3 | 8 | 11 | 16 | 52 |
| 5 | 3 | 3 | 3 | 9 | 14 | 65 |
| 6 | 4 | 4 | 7 | ? | 30 | 78 |
| 7 | 4 | 4 | 5 | ? | 28 | 91 |
| 8 | 4 | 6 | 11 | ? | 58 | 104 |
| 9 | 4 | 5 | 4 | ? | 56 | 117 |
| 10 | 5 | 4 | 10 | ? | 57 | 130 |

Figure 5: Bounds and exact values of sizes of shortest proofs for theorems with up to $t = 8$ symbols

| $t$ | Lower bound | $L(t)$ | Upper bound |
|---|---|---|---|
| 3 | 2 | 4 | 39 |
| 5 | 2 | 9 | 65 |
| 10 | 2 | ? | 130 |
| 100 | 9 | ? | 1300 |
| 1000 | 65 | ? | 13000 |

Figure 6: Bounds on the number $L(t)$ of lines that the proof of a theorem with $t$ symbols must have. The lower bound is from Theorem 4 and the upper bound is $13t$.

It would be also interesting to study shortest proofs if the size of a proof is measured in terms of the number of symbols it contains.

# References


[Ajt94] Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14, 1994.

[Ant97] Luis F. Antunes. Short proofs for MIU theorems. Technical report, Laboratório de Inteligência Artificial e de Ciência de Computadores, Universidade do Porto, 1997. (To be published).

[Bus87] Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52, 1987.

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics (second edition)*. Addison–Wesley, Reading, MA, 1994.

[Hof79] Dougals R. Hofstadter. *Gödel, Escher, Bach, and Eternal Golden Braid*. Penguin, 1979.

[Mat97] Armando B. Matos. The theorems of the formal system MIU. Technical report, Laboratório de Inteligência Artificial e de Ciência de Computadores, Universidade do Porto, 1997.

[PBI93] Pitassi, Beame, and Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3, 1993.

[SR77] S.A. Cook and R.A. Reckhow. The relative complexity of propositional proof systems. *Journal of Symbolic Logic*, 44(1):37–50, 1977.

[Tse68] G. S. Tseitin. On the complexity of derivations in propositional calculus. In A. O. Slisenko, editor, *Studies in Mathematics and Logic, Part II*, pages 115–125. Springer-Verlag, 1992, 1968. (Translated from Russian.

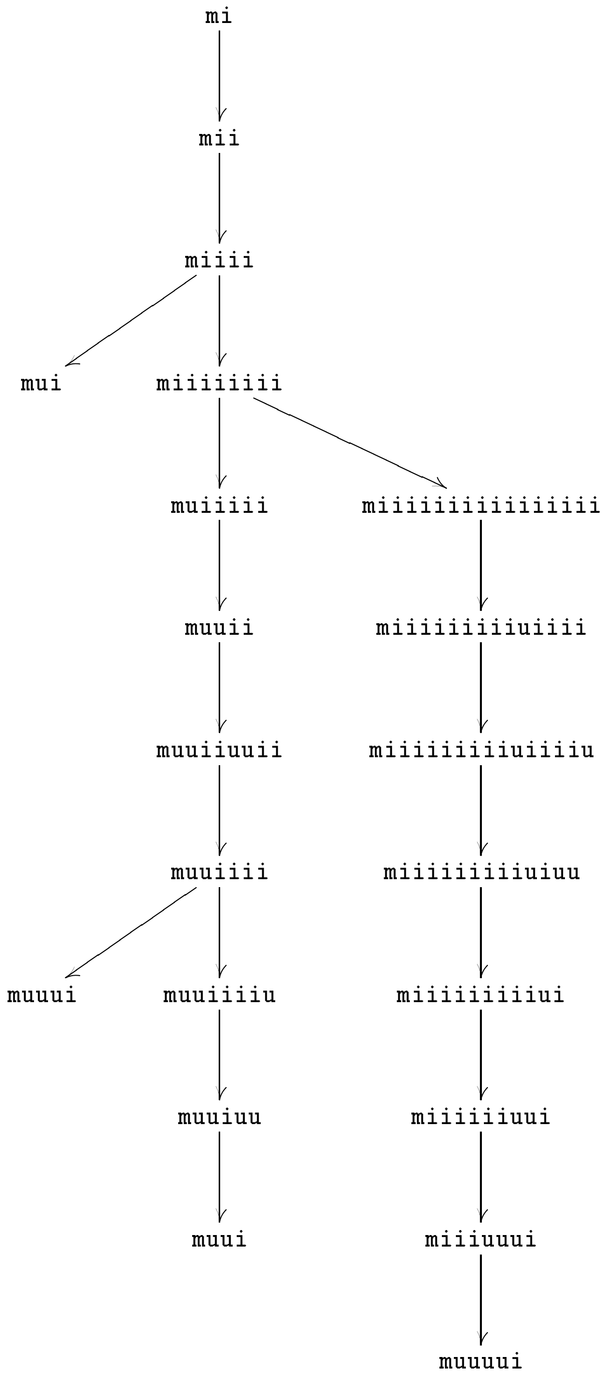


Figure 7: A small part of the MIU graph

[Urq87] Alasdair Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.

[Urq92] Urquhart. Complexity of proofs in classical propositional logic. In *Logic from Computer Science: Proceedings of a Workshop held November 13-17, 1989*. Springer-Verlag, 1992, 1992.