A compact description of finite simple groups

Julien Grange, supervised by Katrin Tent
Universität Münster

Summer 2016

Contents

This paper presents the work I have done under the supervision of Professor Katrin Tent, of the Münster University, as part of my 4-month research internship at the M2-MPRI.

The general context

In their article [1], André Nies and Katrin Tent present a logarithmic description of every simple finite group in first order logic, and a description of every finite group in $\log^3$.

The research problem

Our aim is to give another logarithmic description of finite simple groups, using a different method, namely describing finite groups by their order.

My contribution

I haven't quite reached my first goal. Precisely, I was able to state in logarithmic length that a finite group is a simple group of a given order, but not which one it is (there may be two different finite simple groups of same order).

As explained in the conclusion, from there it should not be too difficult to describe each finite simple group. I couldn't investigate further, for lack of time.

I also gave a (actually, two) logarithmic description of every cyclic group.

Future work

The logical follow-up would be to study the classification of finite simple groups, in order to distinguish the ones that have the same order, in logarithmic length. That way, we could give a short description of every finite simple group.

Also, the logarithmic descriptions of finite groups by their order, and of cyclic groups, could be useful tools to concisely describe other families of finite groups.

1 Introduction and definitions

1.1 Context and goal

We work in the language $\mathcal{L} = (\circ, e)$, where $\circ$ is a binary function symbol, and e is a constant symbol.

For each finite simple group G, we're hoping to give a $\mathcal{L}$-description of G up to isomorphism among the finite groups, that is a $\mathcal{L}$-sentence Φ_G such that for every finite group H, $H \models \Phi_G$ if and only if $H \cong G$.

We would like the length of the sentences $(\Phi_G)_G$ to be in $O(\log |G|)$.

1.2 Caveat

In order not to waste too much time, we won't be totally rigourous, and allow ourselves some shortcuts, such as identifying variables in a formula and the elements they refer to in the model.

For instance, if we define the formula

$$\varphi(x) \quad := \quad \exists y, \quad y \circ y = x$$

we will later allow ourselves to say that ($\mathcal{M}$ beeing a $\mathcal{L}$-structure and x an element of $\mathcal{M}$) $\mathcal{M} \models \varphi(x)$. Of course, here one should read, for instance,

$$\varphi(\dot{x}) \quad := \quad \exists y, \quad y \circ y = \dot{x}$$

and $\mathcal{M}, \dot{x} \to x \models \varphi(\dot{x})$.

Furthermore, we may say something like "Let y be a witness for $\varphi(x)$ in $\mathcal{M}$". This means that we non-constructively pick any element y of $\mathcal{M}$ such that $\mathcal{M} \models y \circ y = x$ (with our previous abuse of notation).

Also, will we use "$\circ$" both as a logic symbol and as the composition law in the groups we consider (although we will write the law "+" in abelian groups).

In any case, what we mean should be clear from the context.

1.3 Definitions

Let's define the logarithm on the integers the same way Nies and Tent do:

Definition 1.1. *For $n < \omega$, $\log n$ denotes the least r such that $2^r \geq n$*

In their paper [1], Nies and Tent define several formulas that we will be using throughout this text. Let us recall them here.

1.3.1 Exponentiation: $\theta_n(g, x)$

First, we want to be able to express concisely that an element of a monoid is a given power of another element. We will do that by quick exponentiation.

Definition 1.2. *Let $n < \omega$, and $n = \overline{a_1 \cdots a_k}^2$ be the binary expansion of n. Let us define the formula $\theta_n(g, x)$ as follows:*

$$\exists y_1, \cdots, y_k, \quad y_1 = x \quad \wedge \quad y_k = g \quad \wedge \quad \bigwedge_{i=1}^{k-1} y_{i+1} = y_i \circ y_i \circ x^{a_{i+1}}$$

where x^ϵ is to be substituted with x if $\epsilon = 1$ and with e otherwise.

Remark. *The formulas $(\theta_n(g, x))_{n<\omega}$ have a length in $O(\log n)$.*

Proposition 1.1. *Let M be a monoid, and $g, x \in M$.*
$M \models \theta_n(g, x)$ iff $g = x^n$ holds in M.

Proof. Suppose that $M \models \theta_n(g, n)$, with witnesses $y_1, \cdots, y_k$. One easily proves by induction on i that $y_i = x^{\overline{a_1 \cdots a_i}^2}$. Thus, $g = x^n$.

Conversely, if $g = x^n$, the elements $y_i = x^{\overline{a_1 \cdots a_i}^2}$ are suitable witnesses for $\theta_n(g, n)$.

□

1.3.2 Exponentiation: $\chi_k(g,n)$

We now want to be able to express that an element is a power of another element, for some power less than 2^k.

Definition 1.3. *Let $k < \omega$. Let us define the formula $\chi_k(g,x)$ as follows:*

$$\exists y_0, \cdots, y_k, \quad y_0 = e \ \wedge \ y_k = g \ \wedge \bigwedge_{i=0}^{k-1} (y_{i+1} = y_i \circ y_i \ \vee \ y_{i+1} = y_i \circ y_i \circ x)$$

Remark. *The formulas $(\chi_k(g,x))_{k<\omega}$ have a length in $O(k)$.*

Proposition 1.2. *Let M be a monoid, and $g, x \in M$.*
$M \models \chi_k(g,x)$ iff $g = x^r$ for some $0 \leq r < 2^k$.

Proof. Suppose that $M \models \chi_k(g,x)$, with witnesses $y_0, \cdots, y_k$. An easy induction on i shows that $y_i = x^r$ for some $0 \leq r < 2^i$. Hence the relation between $g = y_k$ and x.

Conversly, suppose $g = x^r$ for some $0 \leq r < 2^k$, and let $r = \overline{a_1 \cdots a_k}^2$ (here, we don't necessarily have $a_1 = 1$). One can show by induction on i that $y_i = x^{\overline{a_1 \cdots a_i}^2}$ are suitable witnesses for $\theta_k(g,x)$, thus $M \models \theta_k(g,x)$.

□

1.3.3 Generated subgroup: $\alpha_m^k(g, x_1, \cdots, x_m)$

Now, we want to be able to state that an element belongs to the subgroup generated by some other elements.

Definition 1.4. *Let $m < \omega$. By induction on k, we define the formulas $\alpha_m^k(g, x_1, \cdots, x_m)$ as follows:*

$$\begin{cases} \alpha_m^0(g, x_1, \cdots, x_m) & := \quad g = e \quad \vee \quad \bigvee_{j=1}^{m} g = x_i \\ \alpha_m^{k+1}(g, x_1, \cdots, x_m) & := \quad \exists u, v, \quad g = u \circ v \\ & \quad \wedge \quad \forall w, \ (w = u \ \vee \ w = v) \to \alpha_m^k(w, x_1, \cdots, x_m) \end{cases}$$

Remark. *The formulas $(\alpha_m^k(g, x_1, \cdots, x_m))_{m,k<\omega}$ have a length in $O(m+k)$.*

A straightforward induction on k gives us the following lemma:

Lemma 1.1. *Let M be a monoid, and $g, x_1, \cdots, x_m \in M$*
$M \models \alpha_m^k(g, x_1, \cdots, x_m)$ iff g can be written as a product of at most 2^k of the x_i's.

Lemma 1.2. *Let G be a finite group, and $x_1, \cdots, x_m \in G$.*
Every $g \in \langle x_1, \cdots, x_m \rangle$ (the subgroup generated by the x_i's) can be written as a product of less than $|G|$ of the $x_i's$.

Proof. Let $g \in \langle x_1, \cdots, x_m \rangle$.

By definition, g can be written as a product of the x_i's and their inverse. Since G is finite, we have that $x_i^{-1} = x_i^{o(x_i)-1}$.

Thus, g can be written as a product of the x_i's.

Let $g = \prod_{j=1}^{l} a_j$ be such a product (that is, every a_j is one of the x_i's), among those of minimal length. We claim that $l < |G|$.

Otherwise, by the pigeonhole principle, there would be some indexes $0 \leq k < k' \leq l$ such that $\prod_{j=1}^{k} a_j = \prod_{j=1}^{k'} a_j$. So $g = \prod_{j=1}^{k} a_j \circ \prod_{j=k'+1}^{l} a_j$, which is impossible by minimality.

□

Those two lemmas now give us the next proposition:

Proposition 1.3. *Let G be a finite group, $g, x_1, \cdots, x_m \in G$, and $k = \log |G|$.*
$G \models \alpha_m^k(g, x_1, \cdots, x_m)$ iff $g \in \langle x_1, \cdots, x_m \rangle$.

Remark. *Thus, it is possible to express that in a group G, $g \in \langle x_1, \cdots, x_m \rangle$ in $O(m + \log |G|)$.*

2 Baby case: cyclic groups

In a first place, let's take a look at a basic familiy of finite groups: the cyclic groups.

We want to describe each cyclic group in a logarithmic length. That is, we are looking for a family of $\mathcal{L}$-sentence $(\Gamma_n)_{n>0}$ of length in $O(\log n)$ such that a group G is a model of Γ_n iff G is cyclic of order n.

2.1 First solution

In $O(\log n)$, we don't (yet - we will later introduce a sentence that will make this problem trivial) have the granularity needed to express that $g = x^r$ for some $0 \leq r < n$, if n isn't some power of 2.

But asserting that $x^r \neq e$ for any $0 < r \leq 2^{\log n - 1}$ (which we can do in $O(\log n)$) will be enough. We will use the fact that all the proper divisors of n are less or equal than $2^{\log n - 1}$.

Definition 2.1. *Let $k < \omega$.*
We define the formula $\zeta_k(g, x)$ as follows:

$$\exists y, \quad \chi_k(y, x) \quad \wedge \quad g = y \circ x$$

The following is a direct consequence of the proposition 1.2:

Proposition 2.1. *Let M be a monoid, and $g, x \in M$.*
$M \models \zeta_k(g, x)$ iff $g = x^r$ for some $0 < r \leq 2^k$.

Definition 2.2. *Let $n \geq 2$ and $k = \log n$.*
We define the sentence Γ_n as follows:

$$\begin{aligned} \exists x, \quad & \forall g,\ \chi_k(g, x) \\ \wedge \quad & \theta_n(e, x) \\ \wedge \quad & \neg\ \zeta_{k-1}(e, x) \end{aligned}$$

Remark. *The sentences $(\Gamma_n)_{n\geq 2}$ have a length in $O(\log n)$.*

Proposition 2.2. *Let G be a group and $n \geq 2$.*
$G \models \Gamma_n$ iff G is cyclic of order n.

Proof. $(\rightarrow)$ Let $G \models \Gamma_n$, with a witness x.

$G \models \forall g,\ \chi_k(g,x)$ implies that $G = \langle x \rangle$. Let's now prove that $o(x) = n$.

$G \models \theta_n(e,x)$ implies that $o(x)$ divides n. Suppose that $o(x) < n$. Let d be the divisor of n such that $o(x) = \frac{n}{d}$ (under our assumption, $d \geq 2$). We claim that $\frac{n}{d} \leq 2^{k-1}$: otherwise, we would have $n > d2^{k-1} \geq 2^k$, which is absurd, since $k = \log n$.

Hence $0 < o(x) \leq 2^{k-1}$, which contradicts $\neg\ \zeta_{k-1}(e,x)$. Thus, $o(x) = n$, and G is cyclic of order n.

$(\leftarrow)$ Let $G = \langle x \rangle$ be a cyclic group of order n. We claim that x is a suitable witness for Γ_n.

$o(x) = n$, thus $G \models \theta_n(e,x)$.

Since x generates G, every $g \in G$ is equal to x^r for some $0 \leq r < n$, and *a fortiori* for some $0 \leq r < 2^k$. Hence $G \models \forall g,\ \chi_k(g,x)$.

$o(x) = n > 2^{k-1}$, thus for every $0 < r \leq 2^{k-1}$, $x^r \neq e$. Hence $G \models \neg\ \zeta_{k-1}(e,x)$.

□

2.2 A cleaner description

The first description we gave of cyclic groups, though correct, wasn't really elegant. We give here another family of sentences $(\Gamma_n)_{n>0}$ that fits the same purpose as the precedent, but is more pleasing.

Furthurmore, it allows us to introduce Sylow p-subgroups, which will be useful when we describe finite groups by their order.

Definition 2.3. *Consider $n > 0$, whose prime decomposition is $\prod\limits_{i=1}^{k} p_i^{a_i}$.*

For $1 \leq i \leq k$, we define the formulas:

$$\sigma_i(x) \quad := \quad \theta_{p_i^{a_i}}(e,x)\ \wedge\ \neg\ \theta_{p_i^{a_i-1}}(e,x)$$

Lemma 2.1. *Let G be a group, and $x \in G$.*
$G \models \sigma_i(x)$ iff $o(x) = p_i^{a_i}$

Definition 2.4. *Let us define Γ_n as follows:*

$$\begin{array}{lll} & \forall x, y, & x \circ y = y \circ x \\ \wedge & \exists x_1, \cdots, x_k, & \bigwedge\limits_{i=1}^{k} \sigma_i(x_i) \\ & & \wedge\ \ \forall g,\ \exists g_1, \cdots, g_k, \quad g = g_1 \circ \cdots \circ g_k \quad \wedge \ \bigwedge\limits_{i=1}^{k} \chi_{\log(p_i^{a_i})}(g_i, x_i) \end{array}$$

Remark. *The family of sentences* $(\Gamma_n)_{n>0}$ *have length in* $O(\sum\limits_{i=1}^{k}\log(p_i^{a_i})) = O(\log n)$.

Theorem 2.1. *Let* G *be a group.*
$G \models \Gamma_n$ *iff* G *is cyclic of order* n.

In order to prove this theorem, we will need the following lemma:

Lemma 2.2. *Let* $k > 0$, *and* $(S_i)_{1\leq i\leq k}$ *be a family of cyclic subgroups of a abelian group* $(G, +)$, *whose orders* $(n_i)_{1\leq i\leq k}$ *are two-by-two coprime.*

Then $\sum\limits_{i=1}^{k} S_i = \bigoplus\limits_{i=1}^{k} S_i \cong S_1 \times \cdots \times S_k$ *is cyclic, of order* $\prod\limits_{i=1}^{k} n_i$

Proof. We prove that by induction on k (the case $k = 1$ being trivial).

First, let's show that $\sum\limits_{i=1}^{k} S_i = \bigoplus\limits_{i=1}^{k} S_i$, that is $S_i \cap \sum\limits_{j\neq i} S_j = \{0\}$, for any $1 \leq i \leq k$.

By the induction hypothesis, we have that $\sum\limits_{j\neq i} S_j$ is cyclic, of order $\prod\limits_{j\neq i} n_j$. Let x be a generator of $\sum\limits_{j\neq i} S_j$, and y be a generator of S_i.

Let $a \in S_i \cap \sum\limits_{j\neq i} S_j$: there exist $r, s < \omega$ such that $a = rx = sy$.

$$n_i a = n_i rx = n_i sy = s(n_i y) = 0$$

Thus $o(x) \mid n_i r$, that is $\prod\limits_{j\neq i} n_j \mid n_i r$. Since n_i and $\prod\limits_{j\neq i} n_j$ are coprime, $\prod\limits_{j\neq i} n_j \mid r$, and $a = rx = 0$

We have shown that $\sum\limits_{i=1}^{k} S_i = \bigoplus\limits_{i=1}^{k} S_i$. Now, it is a general fact that $\bigoplus\limits_{i=1}^{k} S_i \cong S_1 \times \cdots \times S_k$ (the external product).

Now, let's prove that $S_1 \times \cdots \times S_k$ is cyclic. Let $(x_i)_{1\leq i\leq k}$ be a family of generators of $(S_i)_{1\leq i\leq k}$, and let $g = (x_1, \cdots, x_k)$. $o(g) = \bigvee\limits_{i=1}^{k} n_i = \prod\limits_{i=1}^{k} n_i$, thus $o(g) = |S_1 \times \cdots \times S_k|$ and g is a generator of $S_1 \times \cdots \times S_k$.

Hence $\sum\limits_{i=1}^{k} S_i$ is cyclic, of order $\prod\limits_{i=1}^{k} n_i$.

□

We now can prove the theorem 2.1:

Proof. ($\rightarrow$) Let $(G, +)$ be a group satisfying Γ_n. Let $x_1, \cdots, x_k \in G$ be witnesses for Γ_n.

For $1 \leq i \leq k$, let S_i be the subgroup of G generated by x_i. We have $|S_i| = p_i^{a_i}$, and $G = \sum\limits_{i=1}^{k} S_i$.

The lemma 2.2 gives us that $G = \sum\limits_{i=1}^{k} S_i$ is cyclic, of order $\prod\limits_{i=1}^{k} |S_i| = n$.

($\leftarrow$) Let $(G, +)$ be a cyclic group of order n. Obviously, G is abelian.

For the witness $x_1, \cdots, x_k$, we choose respective generators of the p_i-Sylow subgroups S_i of G (which are cyclic too). Then $G \models \sigma_i(x_i)$ for each i.

By the lemma 2.2, $|\sum_{i=1}^{k} S_i| = n$, thus $\sum_{i=1}^{k} S_i = G$. Hence we can decompose each $g \in G$ as a sum of g_i, with each g_i being in S_i, that is such that $G \models \chi_{\log(p_i^{a_i})}(g_i, x_i)$.

□

3 Describing groups by their size

3.1 Frattini subgroup of a p-group

We here recall the definition of the Frattini subgroup:

Definition 3.1. *Let G be a group.*

We define the Frattini subgroup *of G, noted $\Phi(G)$, as the intersection of the maximal proper subgroups of G.*

By convention, if G doesn't admit any maximal proper subgroup, we set $\Phi(G) = G$.

The theorem 3.1 is a known result.

Theorem 3.1. *Let G be a finite p-group.*

$\Phi(G) \lhd G$ (this is true in every group), and there exists $d < \omega$ such that

$$G/\Phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^d$$

Remark. *If G is a finite p-group* other than (e), *there exists at least one maximal subgroup.*

Thus, $\Phi(G) \subsetneqq G$, and $d > 0$.

We will prove the theorem 3.1, for the sake of completeness, and because it is not easy to find a concise proof of it (at least, I couldn't find one). For that, we will use the lemmas 3.2 and 3.3.

Lemma 3.1. *Let G be a p-group of order p^n $(n \geq 1)$ and $M < G$ a maximal proper subgroup.*

Then $M \lhd G$ and $[G : M] = p$.

Proof. We prove the lemma by induction on n. If $n = 1$, then G is cyclic of order p, and $M = (e)$ is normal, of index p. Now, the inductive case:

It is a well-known fact that since G is a p-group, the center $Z(G)$ isn't trivial. Cauchy's theorem then gives us the existence of a $z \in Z(G)$ of order p.

- if $z \in M$, then it is easy to show that $M/\langle z\rangle$ is a maximal proper subgroup of $G/\langle z\rangle$.

  By induction hypothesis (since $G/\langle z\rangle$ is a p-group of order p^{n-1}), $M/\langle z\rangle$ is a normal subgroup of $G/\langle z\rangle$, of order p^{n-2} (since it is of index p).

  From there, it is easy to show that M is normal in G. And $|M| = p^{n-1}$ implies $[G : M] = p$.

- if $z \notin M$, we claim that $M\langle z\rangle = G$. This amounts to proving that $M\langle z\rangle$ is a subgroup, by maximality of M. We get that because z commutes with every $m \in M$.

We now claim that $M \lhd G$: let $x \in M$ and $mz^k \in G = M\langle z \rangle$.

$$(mz^k)x(mz^k)^{-1} = mxm^{-1} \in M$$

Hence $M \lhd G$.

Now, since $G/M = \{\bar{z^k} : 0 \leq k < p\}$, $[G : M] = p$.

□

Lemma 3.2. *Let G be a finite p-group.*
$G/\Phi(G)$ is abelian.

Proof. We will use the well-known fact that for any $H \lhd G$, G/H is abelian iff $D(G) < H$.

Let M a maximal proper subgroup of G. The lemma 3.1 gives us that G/M is an abelian group (since it is cyclic), thus $D(G) < M$.

Hence, $D(G) < \Phi(G)$ and $G/\Phi(G)$ is an abelian group. □

Lemma 3.3. *Let G be a p-group of order p^n.*
Every $h \in G/\Phi(G)$ is such that $h^p = e$.

Proof.

- First of all, we claim that for every $g \in G$, $g^p \in \Phi(G)$.

  Let M be a maximal proper subgoup of G. From lemma 3.1, we get that $|G/M| = p$.

  Let us consider the canonical surjective morphism $\pi_M : G \rightarrow G/M$: for every $g \in G$, $\pi_M(g^p) = (\phi_M(g))^p = e$, thus $g^p \in M$.

  Hence, $\forall g \in G,\ g^p \in \Phi(G)$.

- Now, consider the canonical surjective morphism $\pi : G \rightarrow G/\Phi(G)$.

  Let $h \in G/\Phi(G)$: there exists some $g \in G$ such that $h = \pi(g)$.

  From there, $h^p = \pi(g^p) = e$, because $g^p \in \Phi(G)$.

□

We now have the tools to prove the theorem 3.1:

Proof.

- First, let's prove that $\Phi(G) \lhd G$. We will prove a stronger result: that G is characteristic, that is stable under every automorphism of G (thus *a fortiori* under every interior automorphism).

  It is easy to see that every automorphism on G induces a permutation on the set of maximal proper subgroups. Hence $\Phi(G)$ is stable under every automorphism.

- By lemma 3.2, we know that $G/\Phi(G)$ is an abelian finite group. The structure theorem for abelian finite groups gives us that

  $$G/\Phi(G) \ \cong\ (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_d^{a_d}\mathbb{Z})$$

  for some primes p_i, and some $a_i > 0$.

  Now, by lemma 3.3, we know that every non-neutral element has order p. This means that for every $1 \leq i \leq d$, $p_i = p$ and $a_i = 1$.

  Hence $G/\Phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^d$.

□

From there, we get the following theorem:

Theorem 3.2. *Let G be a finite p-group, of order p^n.*

There exists $x_1, \cdots, x_n$ such that every $g \in G$ can be written

$$g = x_1^{a_1} \circ \cdots \circ x_n^{a_n} \quad ; \quad 0 \leq a_i < p$$

Such a decomposition is unique (once we've fixed the x_i's).

We'll say that $x_1, \cdots, x_n$ p-generate G.

Proof. First, notice that if such a decomposition exists for every $g \in G$, it is unique, since there are p^n possible decompositions, and $|G| = p^n$.

Let's prove the existence of p-generators $x_1, \cdots, x_n$ by induction on n (the case $n = 0$ beeing trivial).

Let $\pi : G \to G/\Phi(G)$ be the natural surjective projection.

We know that since G is a finite p-group, $G/\Phi(G)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^d$, for some $0 < d \leq n$. Let's pick some $x_1, \cdots, x_d$ in G such that $\pi(x_i) = (0, \cdots, \underbrace{1}_{i}, \cdots, 0)$.

$\Phi(G)$ is a finite p-group of size p^{n-d} and $n - d < n$, thus, by our induction hypothesis, we can find $x_{d+1}, \cdots, x_n$ in $\Phi(G)$ that p-generate $\Phi(G)$.

Now, let's prove that $x_1, \cdots, x_n$ p-generate G. Let $g \in G$.

$\pi(g) \in G/\Phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^d$, so $\pi(g) = \prod\limits_{i=1}^{d} \pi(x_i)^{a_i}$, for some $(0 \leq a_i < p)_{1 \leq i \leq d}$.

Since π is an homomorphism, $\pi(g) = \pi(\prod\limits_{i=1}^{d} x_i^{a_i})$, hence there exists $h \in \Phi(G)$ such that $g = \prod\limits_{i=1}^{d} x_i^{a_i}\ h$.

Since $h \in \Phi(G)$, $h = \prod\limits_{i=d+1}^{n} x_i^{a_i}$, for some $(0 \leq a_i < p)_{d+1 \leq i \leq n}$, and thus $g = \prod\limits_{i=1}^{n} x_i^{a_i}$, where $(0 \leq a_i < p)_{1 \leq i \leq n}$.

Hence $x_1, \cdots, x_n$ p-generate G.

□

3.2 Describing p-groups

For p prime and $n < \omega$, we want to find a $\mathcal{L}$-sentence $\Psi_{p,n}$ such that a group G is a model of $\Psi_{p,n}$ iff G is a p-group of order p^n.

We would our family of sentences $(\Psi_{p,n})_{p,n}$ to be of length in $O(\log(p^n))$.

The paper from Nies and Tent provides us (definition 1.3) with a formula $\chi_k(g, x)$ in $O(k)$ such that if M is a monoid and g, x are two elements of M, $M \models \chi_k(g, x)$ iff $g = x^r$ for some $0 \leq r < 2^k$.

If we want to describe groups of size p^n in $O(\log(p^n))$, we need to be able to be more precise, and to state concisely (in $O(\log q)$) that $g = x^i$ for some $0 \leq r \leq q$, not only when q is some $2^k - 1$.

Definition 3.2. *Let $q < \omega$ and $q = \overline{a_1 \cdots a_k}^2$.*
We define $\phi_q(g,x)$ as follows:

$$\begin{array}{lll}
& & \exists y_0, \cdots, y_k,\ \exists z_0, \cdots, z_k, \quad y_0 = e \quad \wedge \quad z_0 = e \quad \wedge \quad y_k = g \\
\wedge & \displaystyle\bigwedge_{0 \le i < k,\ a_{i+1}=0} & [\ y_{i+1} = y_i \circ y_i \quad \wedge \quad (z_{i+1} = e \leftrightarrow z_i = e) \\
& & \vee \quad z_i \neq e \quad \wedge \quad y_{i+1} = y_i \circ y_i \circ x \quad \wedge \quad z_{i+1} \neq e\ ] \\
\wedge & \displaystyle\bigwedge_{0 \le i < k,\ a_{i+1}=1} & [\ y_{i+1} = y_i \circ y_i \quad \wedge \quad z_{i+1} \neq e \\
& & \vee \quad y_{i+1} = y_i \circ y_i \circ x \quad \wedge \quad (z_{i+1} = e \leftrightarrow z_i = e)\ ]
\end{array}$$

Remark. *The formulas $(\phi_q(g,x))_{q<\omega}$ have a length in $O(\log q)$.*

Proposition 3.1. *Let M be a moinoid, and $g, x \in M$.*
$M \models \phi_q(g,x)$ iff $g = x^r$ for some $0 \le r \le q$

Remark. *The z_i can be thought of as witnesses. Intuitively, $z_i = e$ holds iff until the i-th step, we have stayed* on the edge *(that is we've applied the rule "$y_{i+1} = y_i \circ y_i$" when $a_{i+1} = 0$, and the rule "$y_{i+1} = y_i \circ y_i \circ x$" when $a_{i+1} = 1$).*

If at the i-th step we have $a_{i+1} = 1$ but we set $y_{i+1} = y_i \circ y_i$, that is we loose *the power, then we set $z_{i+1} \neq e$, and from there, for $j > i$, we set $z_j \neq e$, and we can have $y_{j+1} = y_j \circ y_j$ or $y_{j+1} = y_j \circ y_j \circ x$, no matter what a_j is, for we know that we'll end up with a power smaller that q.*

Let's now formally prove the proposition 3.1:

Proof. ($\rightarrow$) Let $M \models \phi_q(g,x)$, with witnesses $y_0, \cdots, y_k, z_0, \cdots, z_k$.

We show by induction on i that:

$$\begin{cases} z_i = e \quad \rightarrow \quad & y_i = x^{\overline{a_1 \cdots a_i}^2} \\ z_i \neq e \quad \rightarrow \quad & \exists\ r_i < \overline{a_1 \cdots a_i}^2, \quad y_i = x^{r_i} \end{cases}$$

For $i = 0$, $z_0 = e$, and $y_0 = x^0$

Let $i < k$. We distinguish two cases, depending on the value of a_{i+1}:

- if $a_{i+1} = 0$
  - if $z_i = e$, then necessarily $z_{i+1} = e$.
    By induction hypothesis, $y_i = x^{\overline{a_1 \cdots a_i}^2}$, thus
    $$y_{i+1} = y_i \circ y_i = x^{\overline{a_1 \cdots a_i 0}^2} = x^{\overline{a_1 \cdots a_i a_{i+1}}^2}$$
  - if $z_i \neq e$, then necessarily $z_{i+1} \neq e$.
    By induction hypothesis, there exists $r_i < \overline{a_1 \cdots a_i}^2$ such that $y_i = x^{r_i}$.
    Either $y_{i+1} = y_i \circ y_i$ or $y_{i+1} = y_i \circ y_i \circ x$. We respectively set $r_{i+1} = 2r_i$ and $r_{i+1} = 2r_i + 1$.
    Obviously, $y_{i+1} = x^{r_{i+1}}$, and $r_i \le \overline{a_1 \cdots a_i}^2 - 1$ implies that, in both cases, $r_{i+1} \le 2r_i + 1 \le \overline{a_1 \cdots a_i 0}^2 - 1$, that is $r_{i+1} < \overline{a_1 \cdots a_i a_{i+1}}^2$

- if $a_{i+1} = 1$
  - $*$ if $z = e$, by induction hypothesis, we have that $y_i = x^{\overline{a_1 \cdots a_i}^2}$
    - $\cdot$ If $z_{i+1} = e$, then necessarily $y_{i+1} = y_i \circ y_i \circ x$.
      Thus $y_{i+1} = x^{\overline{a_1 \cdots a_i 1}^2} = x^{\overline{a_1 \cdots a_i a_{i+1}}^2}$.
    - $\cdot$ If $z_{i+1} \neq e$, then necessarily $y_{i+1} = y_i \circ y_i$.
      Thus, $y_{i+1} = x^{\overline{a_1 \cdots a_i 0}^2}$, and $r_{i+1} = \overline{a_1 \cdots a_i 0}^2$ is such that $r_{i+1} < \overline{a_1 \cdots a_i a_{i+1}}^2$ and $y_{i+1} = x^{r_{i+1}}$.
  - $*$ if $z \neq e$, then by induction hypothesis, there exists $r_i < \overline{a_1 \cdots a_i}^2$ such that $y_i = x^{r_i}$.
    Necessarily, we have that $z_{i+1} \neq e$, and either $y_{i+1} = y_i \circ y_i$ or $y_{i+1} = y_i \circ y_i \circ x$. We set respectively $r_{i+1} = 2r_i$ and $r_{i+1} = 2r_i + 1$.
    Either way, $r_i < \overline{a_1 \cdots a_i}^2$ implies that

    $$r_{i+1} \leq 2r_i + 1 < \overline{a_1 \cdots a_i 1}^2$$

    thus $r_{i+1} < \overline{a_1 \cdots a_i a_{i+1}}^2$.
    In both cases, $y_{i+1} = x^{r_{i+1}}$

Thus, for $i = k$, we have that $g = y_k = x^{\overline{a_1 \cdots a_k}^2}$ or that $g = y_k = x^{r_k}$ for some $r_k < \overline{a_1 \cdots a_k}^2$.

Either way, $g = x^r$ for some $0 \leq r \leq q$.

($\leftarrow$) Suppose that $g = x^r$ for some $0 \leq r \leq q$.

- if $g = x^q$, then we set, for every $0 \leq i \leq k$, $z_i = e$ and $y_i = x^{\overline{a_1 \cdots a_i}^2}$.
  On easily checks that these are suitable witnesses for $\phi_q(g, x)$.
- otherwise, there is a $0 \leq r < q$ such that $g = x^r$.
  Let $z \in M$ be such that $z \neq e$ (since $g \neq x^q$, M is not the trivial monoid, and such a z exists).
  Let $r = \overline{b_1 \cdots b_k}^2$ (here, b_1 isn't necessarily equal to 1).
  Since $r < q$, there exists an $1 \leq i_0 \leq k$ such that,

  $$\begin{cases} \forall i < i_0, \quad b_i = a_i \\ a_{i_0} = 1 \\ b_{i_0} = 0 \end{cases}$$

  We set, for $0 \leq i < i_0$, $z_i = e$ and $y_i = x^{\overline{b_1 \cdots b_i}^2}$,
  and for $i_0 \leq i \leq k$, $z_i = z$ and $y_i = x^{\overline{b_1 \cdots b_i}^2}$.
  One checks that these are suitable witnesses (by a case analysis).

□

Remark. *Now that we've got $\phi_q(g, n)$, it is trivial to describe the cyclic group of order n. For $n \geq 2$, we define Γ_n as follows:*

$$\exists x, \quad \theta_n(e, x) \ \wedge \ \neg \left[\ \exists y, \ \phi_{n-2}(y, x) \ \wedge \ y \circ x = e \ \right] \ \wedge \ \forall g, \ \phi_{n-1}(g, x)$$

Let G be a group. $G \models \Gamma_n$ iff there exists a $x \in G$ that generates G, such that $o(x) = n$ ($o(x)$ divides n, and for all $0 < r \leq n - 1$, $x^r \neq e$).

Hence Γ_n describes in a logarithmic length the cyclic group of order n.

Definition 3.3. *Let us define the sentence $\Psi_{p,n}$ as follows:*

$$\begin{array}{l}
\exists x_1, \cdots, x_n, \quad \forall y, \ \bigwedge_{i=1}^{n} \neg \ [\ \phi_{p-2}(y, x_i) \ \wedge \ y \circ x_i = e \ ] \\
\qquad\qquad \wedge \quad \forall g, \quad \exists g_1, \cdots, g_n, \\
\qquad\qquad\quad [\ \bigwedge_{i=1}^{n} \phi_{p-1}(g_i, x_i) \ \wedge \ g = g_1 \circ \cdots \circ g_n \\
\qquad\qquad\qquad \wedge \quad \forall h_1, \cdots, h_n, \\
\qquad\qquad\qquad\quad (\bigwedge_{i=1}^{n} \phi_{p-1}(h_i, x_i) \ \wedge \ g = h_1 \circ \cdots \circ h_n) \ \rightarrow \ \bigwedge_{i=1}^{n} h_i = g_i \ ]
\end{array}$$

Remark. *The sentences $(\Psi_{p,n})_{p,n}$ have a length in $O(\log(p^n))$.*

Proposition 3.2. *Let G be a group.*
$G \models \Psi_{p,n}$ iff G is a p-group of order p^n.

Proof. ($\rightarrow$) Let G be a group such that $g \models \Psi_{p,n}$, with witnesses $x_1, \cdots, x_n$.

The application f defined as:

$$\begin{array}{rcl}
f: \ \prod_{i=1}^{n} [|0, p-1|] & \rightarrow & G \\
(a_1, \cdots, a_n) & \mapsto & \prod_{i=1}^{n} x_i^{a_i}
\end{array}$$

is bijective. Hence, $|G| = p^n$.

($\leftarrow$) Let G be a p-group of order p^n.

The theorem 3.2 gives us the existence of p-generators $x_1, \cdots, x_n$ of G. These p-generators are suitable witnesses for $\Psi_{p,n}$.

□

3.3 General case

We're looking for a family of $\mathcal{L}$-sentence $(\Omega_n)_{n>0}$ with a length in $O(\log n)$ such that a finite group G is a model of Ω_n iff G has order n.

Definition 3.4. *For $k, m < \omega$, and $g, x_1, \cdots, x_m \in G$, we say that g can be written as a $(x_i)_i^{\pm}$-product of length at most k iff there are $0 \leq l \leq k$ and $a_1, \cdots, a_l \in G$ such that $g = \prod_{j=1}^{l} a_j$ and for all $1 \leq j \leq l$, there exists a $1 \leq i \leq m$ such that $a_j = x_i$ or $a_j = x_i^{-1}$.*

Definition 3.5. *Let us define the formulas $(\beta_m^j(g, x_1, \cdots, x_m))_{j<\omega}$ by induction on j as follows:*

$$\left\{ \begin{array}{lcl}
\beta_m^0(g, x_1, \cdots, x_m) & := & \bigvee_{i=1}^{m} (\ g = x_i \ \vee \ g = e \ \vee \ g \circ x_i = e \ ) \\
 & & \\
\beta_m^{j+1}(g, x_1, \cdots, x_m) & := & \exists u, v, \ \forall w, [(w = u \ \vee \ w = v) \ \rightarrow \ \beta_m^j(w, x_1, \cdots, x_m)] \\
 & & \qquad \wedge \quad g = u \circ v
\end{array} \right.$$

Definition 3.6. *For $m, j < \omega$, we define the formulas*

$$\begin{aligned} \gamma^j_m(g, x_1, \cdots, x_m) \quad := \quad & \exists\, h, a, \quad g = h \circ a \quad \wedge \quad \beta^j_m(h, x_1, \cdots, x_m) \\ & \wedge \quad \bigvee_{i=1}^{m} \ (\ a = x_i \ \vee \ a = e \ \vee \ a \circ x_i = e\ ) \end{aligned}$$

Remark. *The formulas $(\beta^j_m(g, x_1, \cdots, x_m))_{m,j<\omega}$ and $(\gamma^j_m(g, x_1, \cdots, c_m))_{m,j<\omega}$ have a length in $O(m + j)$.*

One can easily prove the following by an induction on j:

Proposition 3.3. *Let G be a group, $m, j < \omega$, and $g, x_1, \cdots, x_m \in G$. We have the following:*

1. *$G \models \beta^j_m(g, x_1, \cdots, x_m)$ iff g can be written as a $(x_i)^{\pm}_i$-product of length at most 2^j*
2. *$G \models \gamma^j_m(g, x_1, \cdots, x_m)$ iff g can be written as a $(x_i)^{\pm}_i$-product of length at most $2^j + 1$*

Definition 3.7. *For p prime and $m < \omega$, let $q = \log(m(p-1))$ let us define the sentence $\Theta_{p,m}$ as follows:*

$$\begin{aligned} \exists x_1, \cdots, x_m, \quad & \forall y, \ \bigwedge_{i=1}^{m} \neg\ [\ \phi_{p-2}(y, x_i) \ \wedge \ y \circ x_i = e\ ] \\ & \wedge \quad \forall g_1, \cdots, g_m, h_1, \cdots, h_m, \\ & \qquad (\ \forall v, \bigwedge_{i=1}^{m} \ [\ (v = g_i \vee v = h_i) \to \phi_{p-1}(v, x_i)\ ] \quad \wedge \quad \prod_{i=1}^{m} g_i = \prod_{i=1}^{m} h_i \ ) \\ & \qquad\quad \to \quad \bigwedge_{i=1}^{m} \ g_i = h_i \\ & \wedge \quad \forall g, \ \gamma^q_m(g, x_1, \cdots, x_m) \ \to \ (\ \beta^q_m(g, x_1, \cdots, x_m) \ \wedge \ \theta_{p^m}(e, g)\ ) \end{aligned}$$

Remark. *The sentences $(\Theta_{p,m})_{p,m}$ have a lenght in $O(\log(p^m) + m)$ (since $q \leq \log(p^m)$), that is $O(\log(p^m))$.*

Proposition 3.4. *Let G be a finite group, p a prime and $m < \omega$.*
$G \models \Theta_{p,m}$ iff p^m divides $|G|$.

Proof. $(\leftarrow)$: suppose that p^m divides $|G|$. Then, by Sylow's theorem, there exists a subgroup $S \leq G$ of order p^m.

Since S is a p-group, we have shown that there exist $x_1, \cdots, x_m \in S$ such that every $g \in S$ can be written $\prod_{i=1}^{m} x_i^{a_i}$, with $0 \leq a_i < p$.

Such a decomposition is unique (since $|S| = p^m$), thus the first part of $\Theta_{p,m}$ holds in G.

As for the second part, let $g \in G$ such that $G \models \gamma^q_m(g, x_1, \cdots, x_m)$. Since $x_i \in S$ and S is a subgroup, that implies that $g \in S$, and $g = \prod_{i=1}^{m} x_i^{a_i}$, for some $0 \leq a_i < p$. Thus g can be written as a product of length at most $m(p-1)$ of the x_i's, and *a fortiori* as a $(x_i)^{\pm}_i$-product of length at most $2^{\log(m(p-1))} = 2^q$. Hence $G \models \beta^q_m(g, x_1, \cdots, x_m)$.

Lagrange gives us that $G \models \theta_{p^m}(e, g)$.

$(\rightarrow)$: assume $G \models \Theta_{p,m}$, with witnesses $x_1, \cdots, x_m$.

Let $H = \langle x_1, \cdots, x_m \rangle$. We will prove that p^m divides $|H|$. From there, Lagrange's theorem implies that p^m divides $|G|$.

First, let's show that H is a p-group. Every $g \in H$ can be written as a $(x_i)_i^{\pm}$-product of some length k. Let's show by induction on k that g can be written as a $(x_i)_i^{\pm}$-product of length at most 2^q:

- if $k \leq 2^q$, there's nothing to prove
- if $k = k' + 1 > 2^q$, let $g = h \circ a$ where h can be written as a $(x_i)_i^{\pm}$-product of length k', and a is either a x_i or a x_i^{-1}.

  By induction, h can be written as a $(x_i)_i^{\pm}$-product of length at most 2^q, thus g can be writtent as a $(x_i)_i^{\pm}$-product of lenght at most $2^q + 1$.

  Thus $G \models \gamma_m^q(g, x_1, \cdots, x_m)$, and from the second part of $\Theta_{p,m}$ we get that $G \models \beta_m^q(g, x_1, \cdots, x_m)$, that is g can be written as a $(x_i)_i^{\pm}$-product of lenght at most 2^q.

So every $g \in H$ can be written as a $(x_i)_i^{\pm}$-product of length at most 2^q, and *a fortiori* as such a product of length at most 2^q+1. Hence $G \models \gamma_m^q(g, x_1, \cdots, x_m)$ for every $g \in H$, and we get from the second part of $\Theta_{p,m}$ that $G \models \theta_{p^m}(e, g)$.

Thus, by Cauchy's theorem, $|H| = p^l$ for some $l < \omega$. All we have left to prove is that $l \geq m$: we get that by considering the application

$$\begin{array}{ccc} \prod_{i=1}^{m} [|0, p-1|] & \rightarrow & H \\ (a_1, \cdots, a_m) & \mapsto & \prod_{i=1}^{m} x_i^{a_i} \end{array}$$

which is an injection, because of the first part of $\Theta_{p,m}$.

$|H| \geq p^m$, so p^m divides $|H|$, and $|G|$.

□

Definition 3.8. *Let $n = \prod_{i=1}^{k} p_i^{n_i}$. Let us define the sentence Ω_n as follows:*

$$\begin{array}{cl} & \forall g,\ \theta_n(e, g) \\ \wedge & \bigwedge_{i=1}^{k} (\ \Theta_{p_i, n_i}\ \wedge\ \neg\Theta_{p_i, n_i+1}\ ) \end{array}$$

Remark. *The sentences $(\Omega_n)_{n>0}$ have a length in $O(\log n + \sum_{i=1}^{k} \log(p_i^{n_i})) = O(\log n)$.*

Theorem 3.3. *Let G be a finite group, and $n > 0$.*

$G \models \Omega_n$ iff $|G| = n$.

Proof. $(\rightarrow)$: suppose that $G \models \Omega_n$. From the first part of Ω_n and Cauchy's theorem, we get that the only prime numbers dividing $|G|$ are the p_i's, that is $|G| = \prod_{i=1}^{k} p_i^{m_i}$, for some $m_i < \omega$.

The second part gives us that for every $1 \leq i \leq k$, $p_i^{n_i}$ divides $|G|$ but $p_i^{n_i+1}$ doesn't. That means that $m_i = n_i$, and eventually that $|G| = n$.

($\leftarrow$) : this is an immediate consequence of the previous proposition, and of Lagrange's theorem.

□

4 Describing finite simple groups

Definition 4.1. *Let $n > 0$, and $k = \log(n)$.*
We define the sentence Δ_n as follows:

$$\begin{array}{l}\forall x_1, \cdots, x_k, \\ \quad [\ (\ \exists h, \quad h \neq e \quad \wedge \quad \alpha_k^k(h, x_1, \cdots, x_k)\ ) \quad \wedge \quad (\ \exists g,\ \neg\, \alpha_k^k(g, x_1, \cdots, x_k)\ )\ ] \\ \to [\ \exists h, g, g', \quad g \circ g' = e\ \wedge\ \alpha_k^k(h, x_1, \cdots, x_k)\ \wedge\ \neg\, \alpha_k^k(g \circ h \circ g', x_1, \cdots, x_k)\ ]\end{array}$$

Remark. *The sentences $(\Delta_n)_{n>0}$ have a length in $O(\log n)$.*

Theorem 4.1. *Let G be a finite group of order (less than) n.*
$G \models \Delta_n$ iff G is simple.

We need the following lemma in order to prove this theorem:

Lemma 4.1. *Let G be a finite group of order n.*
There exists a generating set of G of size at most $\log n$.

Proof. Let $\{x_1, \cdots, x_k\}$ be a generating set for G, among those of minimal size (finite generating sets exist, since G itself is finite). Let's prove that $k \leq \log n$.

We prove by induction on i that $|\langle x_1, \cdots, x_i \rangle| \geq 2^i$, the case $i = 0$ beeing trivial.

For the inductive case, suppose that $|\langle x_1, \cdots, x_i \rangle| \geq 2^i$ for some $i < k$.

$x_{i+1} \notin \langle x_1, \cdots, x_i \rangle$, by minimality. This means that

$$\langle x_1, \cdots, x_i \rangle\ \cap\ x_{i+1}\langle x_1, \cdots, x_i \rangle = \emptyset$$

Since both these sets are included in $\langle x_1, \cdots, x_{i+1} \rangle$, by induction hypothesis, we get that $|\langle x_1, \cdots, x_{i+1} \rangle| \geq 2^{i+1}$

We now have that $|\langle x_1, \cdots, x_k \rangle| \geq 2^k$, but since $\langle x_1, \cdots, x_k \rangle \subseteq G$, necessarily $2^k \leq n$, hence $k \leq \log n$.

□

We're now able to prove the theorem 4.1:

Proof. First, note that since we're considering a group G of size at most 2^k, the formula $\alpha_k^k(g, x_1, \cdots, x_k)$ holds exactly when $g \in \langle x_1, \cdots, x_k \rangle$. (see prop. 1.3)

($\rightarrow$) Suppose that $G \models \Delta_n$, and that there exists a proper non-trivial $H \lhd G$.

Then, by lemma 4.1, there exists a generating set of H of size at most k.

This set gives us the witnesses $x_1, \cdots, x_k$ we need to contradict Δ_n (if its size is stricly less that k, then we complete with e's).

Indeed, since H is a proper non-trivial subgroup, Δ_n's premise holds, but its conclusion doesn't, because of H's normality.

Hence such an proper non-trivial normal subgroup H doesn't exist, and G is a simple group.

($\leftarrow$) Suppose that G is simple. We want to show that $G \models \Delta_n$.

Let $x_1, \cdots, x_k \in G$.

If the premise of Δ_n holds in G wrt $x_1, \cdots, x_k$, then it means that $\langle x_1, \cdots, x_k \rangle$ is a proper non-trivial subgroup of G.

By simplicity, $\langle x_1, \cdots, x_k \rangle$ cannot be normal, thus $\Delta's$ conclusion holds in G wrt $x_1, \cdots, x_k$, and $G \models \Delta_n$.

□

Recall the definitions 3.8 and 4.1.

Definition 4.2. *Let $n > 0$. We define the sentence Φ_n as follows:*

$$\Phi_n \quad := \quad \Omega_n \ \wedge \ \Delta_n$$

Remark. *The sentences $(\Phi_n)_{n>0}$ have a length in $O(\log n)$.*

Now comes our ultimate result:

Theorem 4.2. *Let G be a finite group.*
$G \models \Phi_n$ iff G is a simple group of order n.

Proof. This follows directly from the theorems 3.3 and 4.1 □

We must ask of G to be finite.

Indeed, for p a big enough prime, there exists a Tarski monster group for p, that is an infinite group such that every non-trivial proper subgroup is cyclic of order p. Let T_p be such a group. (we set $k = \log p$)

Proposition 4.1. $T_p \models \Phi_p$

This results from the following lemmas:

Lemma 4.2. $T_p \models \forall g, \ \theta_p(e, g)$

Proof. Let $g \neq e$ be an element of T_p.

We claim that g must be of finite order. Otherwise, $\langle g^2 \rangle$ would be an infinite proper subgroup of T_p.

Now, $o(g) = p$, for otherwise $\langle g \rangle$ would be a finite subgroup of order other than p. □

Lemma 4.3. $T_p \models \Omega_p$

Proof. We already know that $T_p \models \forall g, \ \theta_p(e, g)$.

It is fairly obvious that $T_p \models \Theta_{p,1}$ (take as witness any $x \neq e$: we know that it will be of order p).

We have left to prove that $T_p \models \neg \ \Theta_{p,2}$. Let's assume that $T_p \models \Theta_{p,2}$, with witnesses x, y.

First of all, we know that $x \notin \langle y \rangle$ (for otherwise $x^1 \circ y^0 = x^0 \circ y^k$ for some $0 \leq k < p$) and $y \neq e$.

Thus, $\langle x, y \rangle = T_p$. Hence every $g \in T_p$ can be written as a $(x, y)^{\pm}$-product. We show by induction, as in the proof of the proposition 3.4, that it can thus be written as such a product of length at most 2^k. That is absurd, since there are only finitely many values possible for these products, and T_p is infinite.

□

Lemma 4.4. $T_p \models \Delta_p$

Proof. Let $x_1, \cdots, x_k \in T_p$, and $G = \langle x_1, \cdots, x_k \rangle$.

- if $G = (e)$, then Δ_p's premise doesn't hold.
- if $|G| = p$, then we claim that G isn't normal. Indeed, if it were, then for any $x \in T_p \setminus G$, $\langle x \rangle G$ would be a group of order p^2.

  Thus Δ_p's conclusion holds (by virtue of proposition 1.3, since $|G| \leq 2^k$).
- else, $G = T_p$.

  There are only finitely many $g \in T_p$ such that $T_p \models \alpha_k^k(g, x_1, \cdots, x_k)$. Let $h \neq e$ be such an element.

  Consider the group action of T_p on itself by conjugation: we claim that the orbit Ω_h is infinite (which will give us a g such that $T_p \models \neg\, \alpha_k^k(g \circ h \circ g^{-1}, x_1, \cdots, x_k))$

  Indeed, $|\Omega_h| = [T_p : \mathrm{Stab}_h]$, and since Stab_h is a proper subgroup of T_p (for otherwise $h \in Z(T_p)$, and for any $x \in T_p \setminus \langle h \rangle$, $\langle h \rangle \langle x \rangle$ would be a subgroup of order p^2), its index in T_p is infinite.

□

We have proved that there are arbitrarily large values of $n < \omega$ such that there exists a model of Φ_n with is infinite, hence the restriction to finite groups.

5 Conclusion

We have found a family of sentences, namely $(\Phi_n)_{n>0}$, of length in $O(\log n)$, such that among the finite groups, Φ_n describes the simple ones of order n.

We've not quite reached our initial goal, which was to describe in a logarithmic length each finite simple group.

However, finite simple groups are determined up to isomorphism by their order, except for two infinite families that conflict, containing non-isomorphic simple groups of same order. If we're able to differentiate these families in a logarithmic length, then we get a logarithmic description of every finite simple group, among all the finite groups.

References

[1] André Nies and Katrin Tent. Describing finite groups by short first-order sentences. *Israel Journal of Mathematics*, 221:85–115, 2017.