Comparing various proofs of the Novikov-Boone theorem based on rewriting

Matteo Acclavio Directeurs: Prof. Y. Lafont , Prof. L. Tortora de Falco

Introduction: The aim of this paper is to analize two demonstrations of the Novikov-Boone theorem of undecidability of the word problem for groups.

Bokut's demonstration [4] [5] is based on a rewriting system induced by the relations of the defining presentation of the Boone group $G(T, q)$. This new infinite rewriting system is built to be convergent. So, in order to verify if a word W is equal to the letter q, it will suffice to compute the normal form of the word W and compare it with q (since q is in normal form). The undecidability of the word problem for $G(T, q)$ will follow from the undecidability of the word problem for the *special* monoid T, which is an encoding of a Turing machine.

Lafont's demonstration [9] is inspired by Aandreaa and Cohen's [1]. It also use rewriting, but the only essential point is the notion of convergent rewriting system. It uses the undecidability of the halting problem for a particular class of abstract machines called *affine machine*. With some property of the free group F_2 it is possible to associate a local isomorphism to every transition of a machine affine $\mathcal{A}$. By the HNN embedding theorem, the configurations of the machine live in some group $G_{\mathcal{A}}$ where transitions are represented by elements of $G_{\mathcal{A}}$. In that group the word problem is equivalent to accessibility of a fixed configuration from any other one.

UNIVERSITÉ FRANCO ITALIENNE

ce mémoire a été rédigé dans le cadre du "Curiculum binational de master en Logique", financé par l'Université Franco-Italienne (programme Vinci 2009)

Contents

Chapter 1

Some backgrounds

1.1 Group theory

Definition 1 (Transversal set) *Let G be a group and H be a subgroup of G (it will be noted by $H \leq G$) we can define a transversal set $H^{\perp}$ of the cosets of H simply choosing*[1] *a random element of each coset. Two element g and g' will be in the same left coset (right coset) iff $g^{-1}g' \in H$ (iff $g'g^{-1} \in H$).*

Given a subgroup H of G and a set $H^{\perp}$ of representatives of right cosets we have a unique decomposition of each element of G:

Proposition 1 *For every $g \in G$ exist a unique decomposition of $g = hv$ with $h \in H$ and $v \in H^{\perp}$.*

Demonstration: Because H induces a partition on G (given by its right cosets) and $g \in Hg$ there exists a unique $v \in H^{\perp}$ such that $Hg = Hv$. So $h = gv^{-1}$ is an element of H and $g = hv$.

Definition 2 (Subgroup generated by a subset of a group G) *If S a subset of a group G, the subgroup generated by S is $\langle S \rangle_G = \{s_1^{\epsilon_1} \dots s_k^{\epsilon_k} | s_i \in S\}$. A subgroup $H \leq G$ is* finitely generated *if $\exists S \subseteq G$, S finite, such that $H = \langle S \rangle_G$.*

Definition 3 *If $H \leq G$ and $x \in G$, the centralizer of x in H is the subgroup of H consisting of elements which commute with x: $C_H(x) = \{h \in H | xh = hx\}$.*

Definition 4 (Local isomorphism) *A* local isomorphism *of G is an isomorphism $\phi : H \to H'$ between two subgroups H and H' of G. An element $t \in G$* represents *ϕ if $\forall x \in G$, $\phi(x) = txt^{-1}$. A subgroup K ϕ-*invariant *if $\phi(H \cap K) = \phi(H' \cap K)$*

1.2 Monoid presentations

We'll use the standard notation $(\Sigma|\mathcal{R})$ for a presentation of a monoid M where Σ is the alphabet, Σ^* its set of words (1 will denote the empty word) and

[1] We need the axiom of choice if [G:H] is not finite.

$\mathcal{R} \subset \Sigma^* \times \Sigma^*$; in order to view a presentation like a *string rewriting system*[2] the couple (w, w') will be also denoted like the reduction rules $w \to w'$. $M = \langle \Sigma | \mathcal{R} \rangle^+$ means that M is equal to the quotient of Σ^* by the congruency $\leftrightarrow^*_{\mathcal{R}}$ generated by $\mathcal{R}$ (the smallest equivalence relation containing $\mathcal{R}$ and compatible with the multiplication). A presentation it's called finite if Σ and $\mathcal{R}$ are finite sets. A group $G = \langle \Sigma | \mathcal{R} \rangle$ is given by the same quotient it will automatically imply the existence for every elements of $\sigma \in \Sigma$ an single element σ^{-1} (the inverse of σ) such that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1$.

Notation: Given a presentation $(\Sigma|\mathcal{R})$ and two words $v, w \in \Sigma^*$, $v \equiv w$ means that v and w are written with the same letters in the same order and $v =_M w$ means that they are equivalent in the quotient M (if there will not be ambiguity it will be denoted $=$).
Example: $\mathbb{Z} \simeq \langle b|\emptyset\rangle =: F_1$ has a minimal presentation $\langle b\rangle := \langle b|\emptyset\rangle$ like a group and a minimal presentation $(\{b, \bar{b}\}|\mathcal{R}_b = \{(\bar{b}b, 1), (b\bar{b}, 1)\})$ like monoid. If $w \equiv b\bar{b}, w' \equiv \bar{b}b$ so $ww' \equiv b\bar{b}^2 b = 1$.

Notation: Words of an alphabet Σ will be signed with small and capital letters, let $w_1, \ldots, w_n \Sigma^*$ with $W(w_1, \ldots, w_n)$ wil be denoted a word $W \in \Sigma^*$ such that every word is written in therm of $w_1, \ldots, w_n$ i.e. $W \equiv W_1 \ldots W_k$ with $W_j \equiv w_i, \forall 1 \leq j \leq k \exists 1 \leq i \leq n$

It's preferable to continue to distinguish the two equivalences $=$ and $\leftrightarrow^*_{\mathcal{R}}$ because the first is independent from the choice of the presentation while the second depends from the rewriting system chosen. If there is not ambiguity (a unique system is given) or if the systems have the same property booth notation will be used with the same meaning.

Definition 5 *A group is finitely presented if it is a finitely presented monoid.*

It's easy to show that given a finite presentation $\langle \Sigma|\mathcal{R}\rangle$ of a group G it's possible to get its presentation like monoid by $(\Sigma \cup \bar{\Sigma}|\mathcal{R} \cup \mathcal{R}_{inv})$ where, if $\Sigma = \{\sigma_i | i \in I\}$, $\bar{\Sigma} = \{\bar{\sigma}_i | i \in I\}$ and $\mathcal{R}_{inv} = \{(\sigma_i\bar{\sigma}_i, 1), (\bar{\sigma}_i\sigma_i, 1) | i \in I\}$ define the relation that associate to each σ its inverse $\bar{\sigma}$.[3]

Definition 6 (Reductions) *Let $u, v \in \Sigma^*$ and $(r, s) \in \mathcal{R}$, we'll denote an* elementary reduction *with $urv \to_{\mathcal{R}} usv$. If it exist a sequence $u_0, u_1 \ldots u_n$ in Σ^* such that $u_i \to_{\mathcal{R}} u_{i+1}$for all $i = 0 \ldots n-1$ it's defined a* composted reduction *$u_0 \to^*_{\mathcal{R}} u_n$ (exists a* path of reduction *from u_0 to u_n in $(\Sigma|\mathcal{R})$). A word w is* reduced *if there are not word v such that $w \to_{\mathcal{R}} v$. If a word u admit an single reduced word $\widehat{u}$ such that $u \to^*_{\mathcal{R}} \widehat{u}$, $\widehat{u}$ is called its* normal form*.*

Definition 7 (Convergent presentation) *A presentation $(\Sigma|\mathcal{R})$ is* noetherian *if there are not infinite sequence $\{u_i\}_{i \in \mathbb{N}}$ such that $u_i \to_{\mathcal{R}} u_{i+1} \forall i \in \mathbb{N}$. A presentation is convergent if it have the Church-Rosser propriety (confluence): for every u, v, v' such that $u \to^*_{\mathcal{R}} v$ and $u \to^*_{\mathcal{R}} v'$ it exists a unique w such that $v \to^*_{\mathcal{R}} w$ and $v' \to^*_{\mathcal{R}} w$.*

---

[2]see. Appendix A

[3]All the relation in the form (v', w') with $v', w' \in \bar{\Sigma}^*$ will be derivable from $\mathcal{R} \cup \mathcal{R}_{inv}$ because of $\leftrightarrow_{\mathcal{R} \cup \mathcal{R}_{inv}}$ it's compatible with the product.

$$
\begin{tikzcd}
 & u \arrow[dl, "*"'] \arrow[dr, "*"] & \\
v \arrow[dr, "*"'] & & v' \arrow[dl, "*"] \\
 & w &
\end{tikzcd}
$$

Figure 1.1: An example of the confluence of a word

Definition 8 *A* subword w *of a word* v *it's a word (denoted* $w \in sub(v)$*) such that* $v = uwu'$ *exists* $u, u' \in \Sigma^*$ *(*u *and* u' *can be the empty word). The intersection of two subword* u *and* w *of a word* v *is the longest word* v' *such that* $u = u'v'$ *and* $w = v'w'$ *and* $u'v'w'$ *is a subword of* v*, if* $v' = 1$ *the intersection is empty. If* w *is a subword of* v *we say that* v *contains* w*, moreover if* $v = wu$ *(*$v = uw$*)* $\exists u \in \Sigma^*$*,* w *it's a prefix (suffix) of* v*.*

Definition 9 (Critical Peak) *Given a presentation* $(\Sigma|\mathcal{R})$ *a* critical peak *is a word* w *containing two subword* v *and* v' *with non-empty intersection such that* v *and* v' *are respectively the prefix and the suffix of* w *(or* $v = w$ *and* $v' \in sub(w)$*) and* $\{(v, u), (v', u')\} \subseteq \mathcal{R}$*,* $\exists u, u'$*. We'll say that a critical peak* w *is solvable if every path of reduction starting from the word* w *converge to a word* $\tilde{w}$*.*

Definition 10 (Standard presentation of a group) *Let* G *be a group we'll define the* standard presentation of G *the presentation* $(\Sigma_G|\mathcal{R}_G)$ *given by* $\Sigma_G = \{a_x | \, x \in G\}$ *and* $\mathcal{R}_G = \{a_1 \to 1, a_x a_y \to a_{xy} | x, y \in G\}$*.*

Remark 1 *The standard presentation of* G *is convergent.*

Demonstration: The confluence depends of the associativity of the group operation (i.e. $\forall x, y, z \in G,\ x(yz) = (xy)z$ and so $a_{x(yz)} = a_{(xy)z}$): we note that every critical peak is in the following form:

$$
\begin{tikzcd}
 & a_x a_y a_z \arrow[dl] \arrow[dr] & \\
a_{xy} a_z \arrow[d] & & a_x a_{yz} \arrow[d] \\
a_{(xy)z} & = & a_{x(yz)}
\end{tikzcd}
$$

Figure 1.2: A critical peak of the standard presentation of a group G

The termination, instead, is guaranteed by the fact that every reduction reduces the length of a word by one and so the reduced word are the letters and the empty word.

$$w = a_{x_1} a_{x_2} \dots a_{x_n} \to^*_{\mathcal{R}_G} a_{x_1 \dots x_n}$$

Definition 11 (Free Product) *Let* $G = \langle \Sigma_G | \mathcal{R}_G \rangle^+$ *and* $H = \langle \Sigma_H | \mathcal{R}_H \rangle^+$ *it's defined the* free product F *of* G *and* H *(noted by* $F = G * H$*) the monoid of the* *words generated by the elements of G and H. It's presentation it's given by the disjoint union of the presentation of G and H, so $F = \langle \Sigma_G \uplus \Sigma_H | \mathcal{R}_G \uplus \mathcal{R}_H \rangle^+$. F_n will note the free group on n generators $F_n = \langle a_1, \ldots, a_n \rangle = F_{1_1} * \cdots * F_{1_n}$ and F_ω the free group of $\aleph_0$ generators $\{\alpha_n\}_{n\in\mathbb{N}}$.*

Definition 12 (Translation) *Let $(\Sigma|\mathcal{R})$ and $(\Sigma'|\mathcal{R}')$ two presentations of monoids. A* translation *$\bar{\phi} : (\Sigma|\mathcal{R}) \to (\Sigma'|\mathcal{R}')$ is given by a function $\phi : \Sigma \to \Sigma'^*$ such that:*

1. $\forall w \in \Sigma,\ \bar{\phi}(w) = \phi(w)$
2. $\forall \mathfrak{r} = (u, v) \in \mathcal{R},\ \bar{\phi}(\mathfrak{r}) = (\phi(u), \phi(v)) \in \leftrightarrow^*_{\mathcal{R}'}$

This translation define a homomorphism $\hat{\phi} : \langle \Sigma|\mathcal{R}\rangle^+ \to \langle \Sigma'|\mathcal{R}'\rangle^+$

Lemma 1 (Lafont embedding lemma) *Let $(\Sigma|\mathcal{R})$ and $(\Sigma'|\mathcal{R}')$ be two presentations such that:*

- $\Sigma \subseteq \Sigma'$
- $(\Sigma'|\mathcal{R}')$ *is convergent*
- $\mathcal{R} = \{(u, v) \in \mathcal{R}' | u \in \Sigma^*\}$

then the inclusion $\phi : \Sigma \hookrightarrow \Sigma'$ defines a translation $\bar{\phi} : (\Sigma|\mathcal{R}) \to (\Sigma'|\mathcal{R}')$ and $\hat{\phi}$ is injective.

Demonstration: Let $[v]_{\mathcal{R}}$ be the equivalence classes of v with respect to $\leftrightarrow^*_{\mathcal{R}}$, it suffice to prove that $[v]_{\mathcal{R}} = [v]_{\mathcal{R}'} \cap \Sigma^*$

$\subseteq$) Since $\mathcal{R} \subseteq \mathcal{R}'$ if $w \in \Sigma^*$ and $w \leftrightarrow^*_{\mathcal{R}} v$ then $w \leftrightarrow^*_{\mathcal{R}'} v$

$\supseteq$) Let $w \in \Sigma'^*$ such that $w \leftrightarrow^*_{\mathcal{R}'} v$. Then, since $(\Sigma'|\mathcal{R}')$ is convergent, there is $u \in \Sigma'^*$ such that $w \to^*_{\mathcal{R}'} u$ and $v \to^*_{\mathcal{R}'} u$. For every $v \in \Sigma^*$, applying a rewriting rule of $\mathcal{R}'$ to v' we get a word in Σ^*, so that $u \in \Sigma$. If also $w \in \Sigma^*$ then $w \leftrightarrow^*_R v$.

Since $\bar{\phi}$ is well defined and for every $v, w \in \Sigma^*$, $v \leftrightarrow^*_{\mathcal{R}'} w$ iff $v \leftrightarrow^*_{\mathcal{R}}$, $\hat{\phi}$ is an injective homomorphism.

Definition 13 (Local convergence) *Let $\mathcal{T} \subseteq \Sigma^*$ and $P = (\Sigma|\mathcal{R})$ a presentation. P is locally convergent on $\mathcal{T}$ or $\mathcal{T}$-convergent iff*

- *If $v, w \in \mathcal{T}$ and $v \to^*_{\mathcal{R}} w$ so it exists a path of reduction with elements in $\mathcal{T}$*
- *for all $w \in \Sigma^*$ if $w \to_{\mathcal{R}} v$, $w \to_{\mathcal{R}} v'$ and $v \in \mathcal{T}$ so exists a unique normal word $\hat{u} \in \mathcal{T}$ such that $v \to_{\mathcal{R}} \hat{u}$ and $v' \to_R \hat{u}$.*

Definition 14 (Embedding Translation) *An* embedding translation $\bar{\phi} : (\Sigma|\mathcal{R}) \to P' = (\Sigma'|\mathcal{R}')$ *it's a translation such that:*

- *P' is locally convergent on $\phi(\Sigma^*)$*
- *$\exists$ a* control function[4] *$\psi : \Sigma'^* \rightharpoonup \Sigma^*$ compatible with $\leftrightarrow^*_{\mathcal{R}'}$ such that $\forall v \in \Sigma^*$, $\psi(\phi(v)) \leftrightarrow^*_{\mathcal{R}} v$*

[4]it can be a partial function

Lemma 2 (Extended embedding lemma) *If exists a embedding translation $\bar{\phi} : (\Sigma|\mathcal{R}) \to P' = (\Sigma'|\mathcal{R}')$, so exist an homomorphism $\hat{\phi} : \langle\Sigma|\mathcal{R}\rangle^+ \hookrightarrow \langle\Sigma'|\mathcal{R}'\rangle^+$*

Demonstration: We define $\hat{\phi}([w]_{\mathcal{R}}) = [\phi(w)]_{\mathcal{R}'}$ and $\hat{\psi}([v]_{\mathcal{R}'}) = [\psi(v)]_{\mathcal{R}}$. Like in 1 will be necessary to demonstrate $\bar{\phi}([v]_{\mathcal{R}}) = [\bar{\phi}(v)]_{\mathcal{R}'}$

$\subseteq$) since $\bar{\phi}(\mathcal{R}) \subseteq \leftrightarrow^*_{\mathcal{R}'}$ if $w \in \Sigma^*$ and $w \leftrightarrow^*_{\mathcal{R}} v$ then $\bar{\phi}(w) \leftrightarrow^*_{\mathcal{R}'} \bar{\phi}(v)$

$\supseteq$) let $w \in \Sigma^*$ if $\bar{\phi}(w) \leftrightarrow^*_{\mathcal{R}'} \bar{\phi}(v)$ then $w \leftrightarrow^*_{\mathcal{R}} v$. Since $(\Sigma'|\mathcal{R}')$ is locally convergent on $\bar{\phi}(\Sigma^*)$, exists unique $\hat{v} \in \Sigma^*$ such that $\bar{\phi}(v) \to^*_{\mathcal{R}'} \bar{\phi}(\hat{v})$ and $w \to^*_{\mathcal{R}'} \bar{\phi}(\hat{v})$. Since ψ is compatible with $\leftrightarrow^*_{\mathcal{R}'}$ and if $z \in \Sigma^*$ every rewriting rule in the path of reduction from a $\bar{\phi}(z)$ to $\bar{\phi}(\hat{v})$ is in $\bar{\phi}(\mathcal{R})$ (local convergence), so $\bar{\phi}(z) \leftrightarrow^*_{\mathcal{R}'} \bar{\phi}(\hat{v})$ iff $z \leftrightarrow^*_{\mathcal{R}} \psi\bar{\phi}(z) \leftrightarrow^*_{\mathcal{R}} \psi\bar{\phi}(\hat{v}) \leftrightarrow^*_{\mathcal{R}} \hat{v}$.

Definition 15 (Iso-translation) *An* iso-translation *between two presentation $\bar{\phi} : (\Sigma|\mathcal{R}) \to P' = (\Sigma'|\mathcal{R}')$ is an embedding translation such that P' is convergent, $\bar{\phi} : \Sigma \leftrightarrow \Sigma'$ and $\bar{\phi}(\leftrightarrow^*_{\mathcal{R}}) = \leftrightarrow^*_{\mathcal{R}'}$*

Proposition 2 *If exists a iso-translation $\bar{\phi} : (\Sigma|\mathcal{R}) \to (\Sigma'|\mathcal{R}')$, so $M = \langle\Sigma|\mathcal{R}\rangle^+$ and $M' = \langle\Sigma'|\mathcal{R}'\rangle^+$ are isomorph.*

Demonstration: By 2 $M \hookrightarrow M'$. Moreover $\bar{\phi}(\Sigma^*) = \Sigma'^*$ is a bijection with the property $\bar{\phi}(ww') = \bar{\phi}(w)\bar{\phi}(w')$, so an isomorphism.

Definition 16 (Lexico-metric order) *Given an alphabet Σ equipped with an order $<_\Sigma$ ($\alpha =_\Sigma \beta$ means $\alpha \leq \beta \wedge \beta \leq \alpha$), $v = \alpha_{i_1} \cdots \alpha_{i_n}$ and $w = \alpha_{j_1} \cdots \alpha_{j_m}$, it's possible to extend it to a* lexicografic order *on the word:*

$$v <_\Sigma w \Leftrightarrow \exists k \forall h < k(\alpha_{i_h} =_\Sigma \alpha_{j_h} \wedge ((k \leq n \wedge n < m) \to \alpha_{i_k} <_\Sigma \alpha_{j_k}))$$

and also to lexico-metric order*:*

$$v \triangleleft_{(\Sigma,<_\Sigma)} w \Leftrightarrow n < m \text{ or } \exists k \leq n \forall h < k(\alpha_{i_h} =_\Sigma \alpha_{j_h} \wedge \alpha_{i_k} <_\Sigma \alpha_{j_k})$$

Example: Let $\Sigma = \{a, b, c\}$ and with the order $a =_\Sigma b <_\Sigma c$ so $abc <_\Sigma bca$, and $abc \triangleleft bca$ but $aabca <_\Sigma bca$ and $bca \triangleleft aabca$.

Theorem 3 *It exist an embedding of F_ω into F_2*

Demonstration: Like in [9], showing that the family $\{b^n a b^{-n}\}_{n\in\mathbb{Z}}$ is free[5] in the group $F_2 = \langle a, b\rangle$, it's possible to have the embedding translation of $\bar{\phi} : F_\omega \to F_2$ given by $\phi(\alpha_n) = b^n a b^{-n}$ and so the proof by lemma.2.
In order to build a new convergent presentation of

$$F_2 = \langle \Sigma = \{a, \bar{a}, b, \bar{b}\} | \mathcal{R} = \{a\bar{a} \to 1, \bar{a}a \to 1, b\bar{b} \to 1, \bar{b}b \to 1\}\rangle^+$$

suffices to add for every $n > 0$ the superfluous generators[6] given by the relation:

$$a_n = b^n a \bar{b}^n \qquad \bar{a}_n = b^n \bar{a} \bar{b}^n \qquad a_{-n} = \bar{b}^n a b^n \qquad \bar{a}_{-n} = \bar{b}^n \bar{a} b^n$$

The following relation will be derivable for every $n \in \mathbb{Z}$ (nominally $a_0 := a$):

$$a_n\bar{a}_n = 1 \quad \bar{a}_n a_n = 1 \quad b a_n = a_{n+1} b \quad b\bar{a}_n = \bar{a}_{n+1} b \quad \bar{b} a_n = a_{n-1}\bar{b} \quad \bar{b}\bar{a}_n = \bar{a}_{n-1}\bar{b}$$

[5] i.e. there are not relations between the elements
[6] them can be viewed like some abbreviation of some word in F_2

Let $\Sigma_2 = \{b, \bar{b}\} \cup \{a_n, \bar{a}_n\}_{n\in\mathbb{Z}}$, a presentation of F_2 it's given by $\langle \Sigma_2 | \mathcal{R}_2 \rangle$ where $\mathcal{R}_2$ consists of the following reduction rules:

$$a_n\bar{a}_n \to 1 \qquad \bar{a}_n a_n \to 1 \qquad b\bar{b} \to 1 \qquad \bar{b}b \to 1$$

$$ba_n \to a_{n+1}b \qquad b\bar{a}_n \to \bar{a}_{n+1}b \qquad \bar{b}a_n \to a_{n-1}\bar{b} \qquad \bar{b}\bar{a}_n \to \bar{a}_{n-1}\bar{b}$$

Defining the order on Σ_2 given by $\forall n,\ a_n =_{\Sigma_2} a_{n+1} =_{\Sigma_2} \bar{a}_n <_{\Sigma_2} b =_{\Sigma_2} \bar{b}$, is possible to define a lexico-metric order $\lhd$ on Σ_2^*. The rewriting system is so noetherian since for every reduction $w \to_{\mathcal{R}_2} w'$, $w' \lhd w$ and $\lhd$ it's a well-order on Σ_2^*. By this order every reduced word will be in the form $\alpha_1 \ldots \alpha_n \beta_i^k$ with $\alpha_i \in \{a_n, \bar{a}_n\}$ and $\beta \in \{b, \bar{b}\}$ Moreover all the critical picks are solvable:

- For every $(\gamma, \gamma') \in \{(a_n, \bar{a}_n), (\bar{a}_n, a_n), (b, \bar{b}), (\bar{b}, b)\}$

$$\begin{tikzcd} & \gamma\gamma'\gamma \arrow[dl] \arrow[dr] & \\ \gamma & = & \gamma \end{tikzcd}$$

- For every $(\alpha_n, \alpha'_n) \in \{(a_n, \bar{a}_n), (\bar{a}_n, a_n)\}$

$$\begin{tikzcd} & \bar{b}\alpha_n\alpha'_n \arrow[dl] \arrow[ddd] \\ \alpha_{n-11}\bar{b}\alpha'_n \arrow[d] & \\ \alpha_{n+1}\alpha'_{n+1}\bar{b} \arrow[dr] & \\ & \bar{b} \end{tikzcd} \qquad \begin{tikzcd} b\alpha_n\alpha'_n \arrow[dr] \arrow[ddd] & \\ & \alpha_{n+1}b\alpha'_n \arrow[d] \\ & \alpha_{n+1}\alpha'_{n+1}b \arrow[dl] \\ b & \end{tikzcd}$$

- For $(\gamma, \gamma', \delta) \in \{(b, \bar{b}, -1), (\bar{b}, b, +1)\}$

$$\begin{tikzcd} & \gamma\gamma'\alpha_n \arrow[dl] \arrow[ddd] \\ \gamma\alpha_{n+\delta}\gamma \arrow[d] & \\ \alpha_n\gamma\gamma' \arrow[dr] & \\ & \gamma \end{tikzcd}$$

This equivalence it's provable by the existence of a iso-translation $\bar{\phi}' : (\Sigma|\mathcal{R}) \to (\Sigma_2|\mathcal{R}_2)$ given by $\bar{\phi}'(a) = a_0$, $\bar{\phi}'(\bar{a}) = \bar{a}_0$, $\bar{\phi}'(\beta) = \beta$ where $\beta = b, \bar{b}$. The control function ψ' is defined by $\psi'(\beta) = \beta$ and $\psi'(\alpha_n) = b^n \alpha b^{n-1}$ where $\beta = b, \bar{b}$ and $\alpha = a\bar{a}$.

Now it's easy to show that the function $\phi : \Sigma_\omega = \{\alpha_n, \bar{\alpha}_n\}_{n\in\mathbb{Z}} \to \Sigma_2^*$ such that $\phi(\alpha_n) = a_n$ and $\phi(\bar{\alpha}_n) = \bar{a}_n$ give an embedding translation $\bar{\phi} : \langle \Sigma_\omega \rangle \to$

$(\Sigma_2|\mathcal{R}_2)$. Since every word in $\phi(\Sigma_\omega)$ are in $\{a_n, \bar{a}_n\}^*_{n\in\mathbb{N}}$, them are in normal form in $(\Sigma_2|\mathcal{R}_2)$ and it's possible to define $\psi : \Sigma_2^* \to \Sigma_\omega$ inductively on the number of a and $\bar{a}$ N_w in w: if $N_w = 0$ so $\psi(w)$ is not defined. Else $w = B(b, \bar{b})\alpha w'$ $\alpha = a$ or $\bar{a}$, so $\psi(w) = a_n\psi(\beta w')$ where $n =$ (#occurence of b in $B(b, \bar{b})$) $-$ (#occurence of $\bar{b}$ in $B(b, \bar{b})$) and $N_{w'} < N_w$.[7]

$\psi(a_n) = \alpha_n,\ \psi(\bar{a}_n) = \bar{\alpha}_n\ \psi(b) = \psi(\bar{b}) = 1$ that satisfy $\forall w \in \Sigma_\omega,\ \psi(\phi(w)) = w$. So $F_\omega = \langle\Sigma_\omega\rangle \hookrightarrow (\Sigma_2|\mathcal{R}_2) = \langle a, b\rangle = F_2$.

Lemma 4 *$\forall p, q \in \mathbb{Z}, q \neq 0$ the family $\{a_p, b^q\}$ is free in F_2*

Demonstration: Because $\{a, b\}$ is free in F_2 and $ord(b) = \infty$, $\{a, b^q\}$ is free in F_2 (if not it means exists relations between a and b). So $\{a_p, b^q\}$ have to be free because it can be obtained from $\{a, b^q\}$ applying the internal isomorphism $x \to b^p x b^{-p}$.

1.3 Computability theory

Definition 17 (Minsky machine) *A* Minsky machine *is an abstract machine $\mathcal{M}$ consisting of:*

- *Labeled unbounded integer-value register: any labeled register can hold a single non-negative integer*
- *A list of (labeled) sequential instructions in the form[8]:*
  - *$INC(r, j)$ = increase r and go to j*
  - *$JZDEC(r, j, k)$ = if $r = 0$ go to j, else decrease r and go to k*
- *A state register: which hold the label of the instruction to execute. A configuration for a 2- register machine $\mathcal{M}$ is a triple (s, a, b) where a, b represent the integers in registers and s a state. The writing $\mathfrak{s} \to_{\mathcal{M}} \mathfrak{s}'$ ($\mathfrak{s} \to^*_{\mathcal{M}} \mathfrak{s}'$) denote that $\mathcal{M}$ transform a configuration $\mathfrak{s}$ in a configuration $\mathfrak{s}'$ in one step (a finite number of steps). A state $(0, a, b)$ will denote a final state.*

Theorem 5 (Undecidability of $\mathcal{H}alt$ problem for 2-register machine) *There exist a 2-register machine with undecidable $\mathcal{H}alt$ problem*

Definition 18 (Modular machines) *[1] A* modular machine *$\mathcal{M}od$ is defined, fixed an $m \in \mathbb{N}$, by a "set of instruction" (a, b, c, ϵ) of quadruples where $0 \leq a, b \leq m$, $0 \leq c \leq m^2$, $\epsilon = R, L$ (at most one quadruple can begin with the same pair a and b), and an integer $0 < n < m$ to define input and output function. A configuration for $\mathcal{M}od$ is a pair (α, β) where $\alpha = um + a$, $\beta = vm + b$. If no quadruple begins with a, b, (α, β) it's called* terminal, *else $(\alpha, \beta) \to_{\mathcal{M}od} (\alpha', \beta')$ where*

$$(\alpha', \beta') = \begin{cases} (um^2 + c, v) & \text{if } \epsilon = R \\ (u, vm^2c) & \text{if } \epsilon = L \end{cases}$$

[7] ψ is defined only on $\{a_n, \bar{a}_n\}$-word and $\psi(a_n) = \alpha_n$ and $\psi(\bar{a}_n) = \bar{\alpha}_n$

[8] Minsky have formulated different equivalent machine with different form of instructions [?]

The computing function of $\mathcal{A}$ is the partial function $u_{\mathcal{M}od} g_{\mathcal{M}od} i_{\mathcal{M}od} : \mathbb{N} \to \mathbb{N}$ defined by:

$$i_{\mathcal{M}od} : \mathbb{N} \to \mathbb{N}^2 \ , \qquad r \to (\sum b_i n^i, n+1) \ \textit{where} \ r = \sum b_i n^i, \ 0 \le b_i < n$$

$$g_{\mathcal{M}od} : \mathbb{N}^2 \to \mathbb{N}^2 \ , \qquad (\alpha, \beta) \to_{\mathcal{A}}^* (\alpha', \beta'), \qquad (\alpha', \beta') \ \textit{terminal}$$

$$u_{\mathcal{M}od} : \mathbb{N}^2 \to \mathbb{N} \ , \qquad (\alpha', \beta') \to \sum_1^k b_i m^{i-1} \ \textit{where} \ \alpha = \sum b_i m^i, \ 0 \le b_i < n$$

where $k = min\{i|b_i = 0\}$. It is so possible, with a proper encoding, to utilize it to simulate a Turing machine[9].

Theorem 6 (Undecidability of $\mathcal{H}alt$ problem for modular machines) *There exist an affine machine $\mathcal{A}$ such that $\mathcal{H}alt_{\mathcal{A}}$ is undecidable.*

Demonstration: Let T_S a Turing machine computing an recursively enumerable set S. Since is possible to encode its computing by a modular machine, so it exists a modular machine $\mathcal{M}od$ such that it computes S. Then $\mathcal{H}alt_{\mathcal{M}od} \simeq \mathcal{H}alt_{T_s}$ is indecidable.

Definition 19 (Affine machine) *An* affine machine*, fixed an $m \in \mathbb{N}$, is a finite set $\mathcal{A} \subset \mathbb{Z} \times \mathbb{Z}^* \times \mathbb{Z} \times \mathbb{Z}^*$. Every $(p, q, p', q') \in \mathcal{A}$ define an* affine transition *$p + qz \to_{\mathcal{A}} p' + q'z$ ($z \in \mathbb{Z}$).*

Remark 2 *Every 2-register machines $\mathcal{M}$ can be simulated by an affine machine: let (s, a, b) a configuration for $\mathcal{M}$, coding it in the integer $[s, a, b] = s + m2^a3^b$, every transition will be in the form:*

$$\begin{array}{lll} i + mk \to i + 2mk & i + m(2z+1) \to j + m(2z+1) & i + 2mz \to k + mz \\ i + mk \to i + 3mk & i + m(3z+1) \to j + m(3z+1) & i + 3mz \to k + mz \\ & i + m(3z+2) \to j + m(3z+2) & \end{array}$$

so if z, z' are two integer, $z \leftrightarrow_{\mathcal{A}}^* z'$ so z is the code of a configuration iff z' is. Futhermore

$$(s, a, b) \to_{\mathcal{M}} (s', a', b') \ \textit{iff} \ (s, a, b) \leftrightarrow_{\mathcal{M}}^* (s', a', b') \ \textit{iff} \ [s, a, b] \leftrightarrow_{\mathcal{A}}^* [s', a', b']$$

Theorem 7 (Undecidability of equivalence problem for affine machines) *There exists a machine affine $\mathcal{A}$ and an integer m such that the equivalence problem it's undecidable.*

Demonstration: The equivalence problem ask if, given a $z = pm + q \in \mathbb{Z}$, $z \leftrightarrow_{\mathcal{A}}^* m$. Let $\mathcal{M}$ a 2-register machine with undecidable $\mathcal{H}alt$ problem, so the problem of equivalence will correspond to the $\mathcal{H}alt$ problem for $\mathcal{M}$ (is possible to suppose that the final state for $\mathcal{M}$ is $(0, 0, 0)$) since $m = [0, 0, 0]$ and $z = [s_z, a_z, b_z]$ so $z \leftrightarrow_{\mathcal{A}}^* m$ iff $(s_z, a_z, b_z) \leftrightarrow_{\mathcal{M}}^* (0, 0, 0)$.

[9] Starting by a Turing machine T on the alphabet $\{b_i\}_{0 \le i \le n}$ is possible to associate the coding of the tape $r = \sum b_i n^i$, at every state of T a quadruple of $\mathcal{M}od$

Chapter 2

The Higman-Neuman-Neuman Extension Theorem

In order to build groups' extensions with particular combinatorial propriety, it will be useful to use the *HNN-theorem* for the groups.

2.1 HNN extension theorem

Theorem 8 (HNN extension associated with a subgroup) *Let G be a group, $\forall H < G, \exists F > G$ and $b \in F$ such that $H = C_G(b)$.*

2.1.1 HNN extension theorem demonstration Part I: A non convergent presentation of F

In order to demonstrate the theorem, we'll build an "ad hoc" extension F of G and we'll show that exist an element $b \in F$ such that $H = C_G(b)$.
Let $F = \frac{G*\langle b\rangle}{\leftrightarrow_C^*}$ where $\leftrightarrow_C^*$ it's the smallest equivalence relation containing the set $C = \{(bh, h\bar{b})|h \in H\}$. The free product $G*\langle b\rangle$, given the standard presentation of G and the minimal presentation of $\mathbb{Z}$ like monoid[1], $G*\langle b\rangle = \langle\Sigma_G \cup \{b, \bar{b}\}|\mathcal{R}_G \cup \{(b\bar{b}, 1), (\bar{b}b, 1)\}\rangle$, so we have a presentation of $F = \langle\Sigma_F = \Sigma_G \cup \{b, \bar{b}\}|\mathcal{R}_F = \mathcal{R}_G \cup R_b \cup \mathcal{R}_H\}\rangle^+$ where $\mathcal{R}_H = \{(\beta a_h, a_h\beta)|h \in H, \beta \in \{b, \bar{b}\}\}$.

Remark 3 *The presentation $\langle\Sigma_F|\mathcal{R}_F\rangle$ is not convergent.*

Demonstration: We just need to observe the critique peak:

- if the critique pick it's a word of the alphabet of G, it's soluble because it's in the standard presentation of G

[1] see 1.2 pag. 2

- if the critique pick it's a word of the alphabet of $\langle b, \bar{b} \rangle$, it is solvable:

$$\begin{tikzcd} & b\bar{b}b \arrow[dl] \arrow[dr] & \\ b & = & b \end{tikzcd} \qquad \begin{tikzcd} & \bar{b}b\bar{b} \arrow[dl] \arrow[dr] & \\ \bar{b} & = & \bar{b} \end{tikzcd}$$

- if the critique peak contain only the letters of Σ_b and a_h with $h, k \in H$, it's solvable:

$$\begin{tikzcd} b\bar{b}a_h \arrow[ddd] \arrow[dr] & \\ & ba_h\bar{b} \arrow[d] \\ & a_h b\bar{b} \arrow[dl] \\ a_h & \end{tikzcd} \quad \begin{tikzcd} \bar{b}ba_h \arrow[ddd] \arrow[dr] & \\ & \bar{b}a_h b \arrow[d] \\ & a_h \bar{b}b \arrow[dl] \\ a_h & \end{tikzcd} \quad \begin{tikzcd} ba_h a_k \arrow[ddd] \arrow[dr] & \\ & a_h b a_k \arrow[d] \\ & ba_h a_k \arrow[dl] \\ ba_{hk} & \end{tikzcd} \quad \begin{tikzcd} \bar{b}a_h a_k \arrow[ddd] \arrow[dr] & \\ & a_h \bar{b} a_k \arrow[d] \\ & \bar{b}a_h a_k \arrow[dl] \\ \bar{b}a_{hk} & \end{tikzcd}$$

- all the non-solvable peak are all in the form ($\beta \in \Sigma_b$, $h \in H$, $x \in G \setminus H$) :

$$\begin{tikzcd} & \beta a_h a_x \arrow[dl] \arrow[dr] & \\ \beta a_{hx} & \neq & a_h \beta a_x \end{tikzcd}$$

2.1.2 HNN extension theorem demonstration Part II: A convergent presentation of F

Using the Lemma1 is possible to give another presentation of F adding new superfluous generators and new relation. Let fix an $H^\perp$ with $1 \in H^\perp$, we define the superfluous generators $b_v = ba_v$ and $b'_v = \bar{b}a_v$ ($\Sigma_\perp := \{b_v, b'_v | v \in H^\perp\}$).[2] Using the relation of $\mathcal{R}_F$ and the fact that, by the Prop.1, is possible to derivate the following set $\mathcal{R}_\perp$ of relations:

$$\forall v \in H^\perp \qquad b_1 b'_v \to a_v \qquad b'_1 b_v \to a_v$$

$$b_v a_x \to a_h b_w \ \exists! h \in H, w \in H^\perp \text{ such that } vx = hw$$

$$b'_v a_x \to a_h b'_w \ \exists! h \in H, w \in H^\perp \text{ such that } vx = hw$$

Proposition 3 *The presentation $\langle \Sigma_G \cup \Sigma_\perp | \mathcal{R}_G \cup \mathcal{R}_\perp \rangle$ of F' is convergent.*

Demonstration: Like in 3, a critique peak of the alphabet Σ_G or $\{b_1, b'_1\}$ is solvable. The others critique peak are all in the form $\beta_v a_x a_y$ or $b_1 b'_v a_x$ or $b'_1 b_v a_x$. These three kind of critique peak are solvable:

[2] $b_v = ba_v$ and $b'_v = \bar{b}a_v$ essentially means that b_v and b'_v are abbreviation respectively for the words ba_v and $\bar{b}a_v$

$$
\begin{tikzcd}
 & \beta_v a_x a_y \arrow[dl] \arrow[dr, "{vx = kw', k \in H, w' \in H^{\perp}}"] & \\
\beta_v a_{xy} \arrow[dd, "{v(xy) = hw, h \in H, w \in H^{\perp}}"'] & & a_k \beta_{w'} a_y \arrow[d, "{w'y = k'w'', k' \in H, w'' \in H^{\perp}}"] \\
 & & a_k a_{k'} \beta_{w''} \arrow[d] \\
a_h \beta_w & = & a_{kk'} \beta_{w''}
\end{tikzcd}
$$

because $hw = v(xy) = (vx)y = (kw')y = k(w'y) = k(k'w'') = (kk')w''$ and by the lemma 1 $w = w''$ and $h = kk'$.

$$
\begin{tikzcd}
 & b_1 b'_v a_x \arrow[dddl] \arrow[dr, "{vx = hw, h \in H, w \in H^{\perp}}"] & \\
 & & b_1 a_h b'_w \arrow[d] \\
 & & a_h b_1 b'_w \arrow[d] \\
a_v a_x \arrow[d] & & a_h a_w \arrow[d] \\
a_{vx} & = & a_{hw}
\end{tikzcd}
$$

the same for the pick $b'_1 b_v a_x$ changing b_1 with b'_1 and b'_v with b_v.

Remark 4 *Every reduced words of this presentation of F' are in the form $\alpha\beta_1 \dots \beta_n$ with $\alpha \in \Sigma_G \cup \{1\}$, $n \geq 0$ and $\beta_i \in \Sigma_\perp$ ($n \neq 1 \Rightarrow \forall i,\ \beta_i \neq b_1$ and $\beta_i \neq b'$).*

Proposition 4 *$F' = \langle \Sigma_{F'} = \Sigma_G \cup \Sigma_\perp | \mathcal{R}_{F'} = \mathcal{R}_G \cup \mathcal{R}_\perp \rangle \simeq F$.*

Demonstration: By Prop.2 , it suffices to show that an iso-translation from F to F' exists. Let $\phi : \Sigma_F \to \Sigma'_F$ such that $\phi(a_x) = a_x$, $\phi(b) = b$ and $\phi(\bar{b}) = b'_1$ we can define $\bar{\phi}$ and so:

- $\forall \mathfrak{r} \in \mathcal{R}, \bar{\phi}(\mathfrak{r}) \in \leftrightarrow^*_{\mathcal{R}'}$
- exists a control function ψ given by $\psi(a_x) = a_x$, $\psi(b_v) = ba_v$ and $\psi(b'_v) = \bar{b}a_v$
- $\leftrightarrow^*_{\bar{\phi}(\mathcal{R})} = \leftrightarrow^*_{\mathcal{R}'}$

so $\bar{\phi}$ will be an iso-translation and $F \simeq F'$.

2.1.3 HNN extension theorem demonstration Part III: Concluding

It's easy to prove by prop.2 that $F' \geq G$ and $F' \geq \langle b \rangle$ because the functions $id_G : \Sigma_G \to \Sigma'^*_F$ and $id_b : \{b, b' = \bar{b}\} \to \Sigma^*_F$ are embedding translation. It's also evident for construction that $C_G(b) \geq H$. To prove the equality it's sufficient to show that only the elements of H commutes with b. Let $x = hw$ with $h \in H$ and $w \in H^{\perp}$, we have $b_1 a_x \rightarrow_{\mathcal{R}_{F'}} a_h b_w$ and so $ba_x = \psi(b_1 a_x) = \psi(\phi(ba_x)) \rightarrow_{\mathcal{R}_F} \psi(a_h b_w)$. But $a_h b_w$ is reduced and so $\psi(a_h b_w) = a_h b a_w$ is. So $\forall x \in G\ xb = hbw = xb$ iff $x \in H$(i.e. $w = 1$) that mean $C_G(b) = H$.

2.2 HNN extention theorem application

Corollary 9 *If G is finitely presented and H is finitely generated in G, then the HNN-extension F of G associated with H is finitely presented.*

Demonstration: It just needs to change a little bit the construction of F used in the demonstration of Th.8. Let $u_1, \dots u_n \in \Sigma_G$ such that $H = \langle u_1, \dots, u_n \rangle$ since $\forall h \in H,\ h = u_{i_1} \dots u_{i_m},\ \exists m > 0$ and $i_j \in \{1, \dots, n\}$. F will be presented by $\langle \Sigma_G \cup \{b, \bar{b}\} | \mathcal{R}_G \cup R_{gen} \rangle$ where $R_{gen} = \{b\bar{b} \rightarrow 1, \bar{b}b \rightarrow 1, bu_1 \rightarrow u_1 b, \dots, bu_n \rightarrow u_n b\}$. By the transitive and operation-compatible closure of R_{gen}, $\forall h \in H$ the relation $(a_h b, ba_h) \in \leftrightarrow^*_{\mathcal{R}_{gen}}$ so $\leftrightarrow^*_{\mathcal{R}_F} \subseteq \leftrightarrow^*_{\mathcal{R}_G \cup \mathcal{R}_{gen}}$ where $\mathcal{R}_F := \mathcal{R}_G \cup \{(hb, bh) | h \in H\}$. Moreover every u_i are elements of H so $R_{gen} \subseteq \mathcal{R}_F$ and $\leftrightarrow^*_{\mathcal{R}_G \cup \mathcal{R}_{gen}} \subseteq \leftrightarrow^*_{\mathcal{R}_F}$.

Theorem 10 (HNN extension associated with an local isomorphism) *Let G be a group, $\forall \phi : H \rightarrow H'$ local isomrphism, $\exists F > G$ and $b \in F$ such that:*

1. *b represents ϕ*
2. *$\langle K, b \rangle_F \cap G = K$ for all K ϕ-invariant*
3. *if G is finitly presented and H finitely generated F is finitely presented*

Demonstration: Let $F = \frac{G * \langle b \rangle}{\leftrightarrow^*_C}$ where $\leftrightarrow^*_C$ is the smallest equivalence relation containing the set $C = \{(bh, \phi(h)b) | h \in H\}$. Fixed $H^{\perp}, H'^{\perp}$ transversal set respectively of cosets of H and H' ($1 \in H^{\perp}$ and $1 \in H'^{\perp}$) is possible to give the following convergent presentation of $F = (\Sigma_{\phi} | \mathcal{R}_{\phi})$ built in the similar way of 2.1.2 ($b_u = ba_u$ and $b'_v = \bar{b}a_v$):

$$\Sigma_{\phi} = \{a_x\}_{x \in G} \cup \{b_u\}_{u \in H^{\perp}} \cup \{b'_v\}_{v \in H'^{\perp}}$$

and the following rewriting rules $\mathcal{R}_{\phi}$

$$a_x a_y \rightarrow a_{xy} \qquad a_1 \rightarrow 1 \qquad b_1 b'_v \rightarrow a_v \qquad b'_1 b_u = a_u$$

$$b_v a_x \rightarrow a_{\phi(h)} b_w \qquad \exists! h \in H, v, w \in H^{\perp} \text{ such that } vx = hw$$

$$b'_v a_x \rightarrow a_{\phi(h')} b'_w \qquad \exists! h' \in H', v, w \in H^{\perp} \text{ such that } vx = h'w$$

Like in Th.8 $(\Sigma_{\phi} | \mathcal{R}_{\phi})$ is a convergent presentation and F is an extension of G and $\langle b \rangle$.
1) b represents ϕ since $\forall u \in H,\ b_1 a_u b'_1 = a_{\phi(u)}$.
2) For every $K < G$ is possible to choose the elements of $H^{\perp}$ and $H'^{\perp}$ such that for every $k \in K$, $k = hv$ where $h \in K \cap H$ and $v \in K \cap H^{\perp}$, under that conditions if K is ϕ-invariant if a word is written in the alphabet

$$\Sigma_{\phi}|_K = \{a_k\}_{k \in K} \cup \{b_u\}_{u \in H^{\perp} \cap K} \cup \{b'_v\}_{v \in H'^{\perp} \cap K}$$

so it is a normal form since every K is a subgroup. That means $\langle K, b \rangle_F \cap G \subseteq K$ and so the equality while $K \subseteq \langle K, b \rangle_F \cap G$.
3) Follow from Cor.9.

Theorem 11 (HNN extension associated with several local isomorphism) *Let G be a group, $\forall \phi_1 : H_1 \to H'_1, \ldots, \phi_n : H_n \to H'_n$ local isomorphism, $\exists F > G$ and $b \in F$ such that:*

1. *b_i represents ϕ_i $\forall i$*
2. *$\langle K, b_1, \ldots, b_n \rangle_F \cap G = K$ for all K invariant for all ϕ_i*
3. *if G is finitely presented and all H_i finitely generated F is finitely presented*

Demonstration: Induction on the number of local isomorphism n using Th.10

Chapter 3

Novikow-Boone's groups

Independently of Higman, Neumann and Neumann's work oriented to a purely algebraic and topological application, Novikow in [12] discover the HNN-extension and approach the subject in a more constructive way. With Boone [6] they connect it to algorithmic and combinatorial algebra demonstrating the undecidability of the word problem for the groups.

3.1 A Novikov-Boone's group zoo

Here will be presented some Novikov-Boone's groups, stating some their properties that permits to demonstrate the undecidability of word problem.

3.1.1 Novikow group $\mathfrak{A}_{p_1,p_2}$

Let K a Post system[1] $[\Sigma_a; \mathcal{R}]$ on the alphabet $\Sigma_a = \{a_1, \ldots, a_n\}$ and $\mathcal{R} = \{(A_i, B_i), 1 \leq i \leq \lambda\}$, A_i, B_i nonempty, is possible to build the Novikow group $\mathfrak{A}_{p_1,p_2}$ associated with K on the alphabet Σ consisting of

$$a_1, \ldots, a_n, q_1, \ldots, q_\lambda, r_1, \ldots, r_\lambda, l_1, \ldots, l_\lambda$$

one of his copy, namely

$$a_1^+, \ldots, a_n^+, q_1^+, \ldots, q_\lambda^+, r_1^+, \ldots, r_\lambda^+, l_1^+, \ldots, l_\lambda^+$$

and two *supporting letters* p_1, p_2 defined by the following relations:

1. $q_i a = a q_i q_i \qquad q_i^+ q_i^+ a^+ = a^+ q_i^+$
2. $r_i r_i a = a r_i \qquad r_i^+ a^+ = a^+ r_i^+ r_i^+$
3. $a l_i = l_i a \qquad a^+ l_i^+ = l_i^+ a^+$
4. $q_i^+ l_i^+ p_1 l_i q_i = A_i^+ p_1 A_i$
5. $r_i^+ p_1 r_i = p_1$
6. $r_i l_i p_2 l_i^+ r_i^+ = B_i p_2 B_i^+$

[1] see. Appendix A

7. $q_i p_2 q_i^+ = p_2$

for $1 \leq i \leq \lambda, a \in \Sigma_a$ and $(a_{s_1}, \ldots, a_{s_k})^+ = a_{s_1}^+, \ldots, a_{s_k}^+$

Proposition 5 (Novikow property) *The words $p_1 X p_2 X^+$ and $p_1 Y p_2 Y^+$ are conjugate in the group $\mathfrak{A}_{p_1 p_2}$ iff $X \sim_K Y$ in the associated Post system K where $X, Y \in \Sigma_a$*

3.1.2 Novikow group $\mathfrak{A}_p$

Let $\Sigma_a = \{a_1, \ldots, a_n\}$ and (A_i, B_i) pairs of nonempty Σ_a-word for $1 \leq i \leq m$.

$$A_{d\mu l\rho} = \langle \Sigma_a \cup \{\rho, \tilde{\rho}, \mu_{1i}, \tilde{\mu}_{1i}, \mu_{2i}, \tilde{\mu}_{2i}, l_{ai}, d_i\}_{1 \leq i \leq m} | \mathcal{R} \rangle$$

where $\mathcal{R}$ is the set of the following relation

1. $\rho_i a = a\rho_i^2 \qquad \tilde{\rho}_i a = a\tilde{\rho}_i^2$
2. $bl_{ai} = l_{ai} b$
3. $a\mu_{1i} lai = \mu_1 ia \qquad a\tilde{\mu}_{1i} lai = \tilde{\mu}_1 ia$
4. $al_{ai}\mu 2i = \mu_{2i} a \qquad al_{ai}\tilde{\mu} 2i = \tilde{\mu}_{2i} a$
5. $\tilde{\mu}_{1i}\tilde{\rho}_i d_i \tilde{\mu}_{2i} = \tilde{\mu}_{1i}\rho_i d_i \tilde{\mu}_{2i} A_i^{-1} B_i$
6. $ad_i = d_i a$

for $1 \leq i \leq \lambda$ and $a, b \in \Sigma_a$.

$$\mathfrak{A}_p = \frac{A_{d\mu l\rho} * A_{d\mu l\rho}^+ * p}{\leftrightarrow_{\mathcal{R}_p}^*}$$

where $A_{d\mu l\rho}^+$ is an antiisomorphic copy of $A_{d\mu l\rho}$ given by the antiisomorphism [2] $x \to x^+$ and $\mathcal{R}_p = \{EpE^+ \to p\}$ where $E \in A_{d\mu l\rho}$.

3.1.3 Boone group

Let $T = (\Sigma_T = \{s_d, q_e\}_{d \in D, e \in E} | \mathcal{R}_T = \{A_i \to B_i, \}_{1 \leq i \leq N})$ with $q_1 = q$, a monoid with A_i, B_i *special words* in the alphabet Σ_a (i.e. word in the form $sq_e s'$ with s, s' words of the alphabet $\{s_d\}$), the Boone group $G(T, q)$ with corresponding monoid T is given by the alphabet

$$\Sigma = \{s_d, q_e, x, y, l_i, r_i, k, t\}_{d \in D, e \in E,\ 1 \leq i \leq N}$$

and the following relations:

1. $y^2 s_d = s_d y \qquad xs_d = s_d x^2$
2. $s_d l_i = yl_i ys_d \qquad s_d xr_i x = r_i s_d$
3. $l_i B_i r_i = A_i$
4. $l_i t = tl_i \qquad yt = ty$

[2]an antiisomorphisme $\phi : G \to G'$ is a map such that $\phi(1_G) = 1_{G'}$ and $\phi(xy) = \phi(y)\phi(x)$

5. $r_i k = k r_i \qquad xk = kx$
6. $q^{-1}tqk = kq^{-1}tq$

Proposition 6 (Boone property) *Let S, S' special words of Σ_a, than $S \leftrightarrow^*_{R_T} S'$ iff $\exists V(l_i, y), W(r_i, x)$ such that $S = V(l_i, y)S'W(r_i, x)$ in $G(T, q)$*

3.1.4 Borisov group

Let $\Sigma_a = \{s_j\}_{1 \le j \le n}$ and $\mathcal{R}_\Pi = \{(F_i, G_i), 1 \le i \le m\}$ a set of pairs of nonempty words of Σ_a and P a fixed arbitrary word of Σ_a. The Borisov group $G(\Pi, P)$ can be presented by the alphabet

$$\Sigma = \Sigma_a \cup \{d, e, c, t, k\}$$

and the following relation

1. $d^{m+1}s = sd \qquad es = se^{m+1}$
2. $sc = cs$
3. $d^i F_i e^i c = cd^i G_i e^i$
4. $ct = tc \qquad dt = td$
5. $ck = kc \qquad ek = ke$
6. $P^{-1}tPk = kP^{-1}tP$

for every $1 \le i \le m$, $s \in \Sigma_a$. Let $\Pi = (\Sigma_a | \mathcal{R}_\Pi)$ the monoid associated with $G(\Pi, P)$.

Proposition 7 (Borisov property) *Let Q be a Σ_a-word then $Q = P$ in the associated monoid iff $Q^{-1}tQk = kQ^{-1}tQ$ in $G(\Pi, P)$.*

3.1.5 Aandrea group

In [5] its presentation is linked with Aandrea's modular machine instruction set [1]. It's presented by an integer $m > 0$ and a set of triples of integer $M = \{(s_i, a_i, b_i)\}_{i \in I} \cup \{(s_j, a_j, b_j)\}_{j \in J}$ where $0 \le a_k, b_k < m$ and $0 \le c_k < m^2$ for every $k \in I \cup J$.

$$G(M) = (r_i, l_j, x, y, t, r, , k; i \in I, j \in J | \mathcal{R}_M)$$

where, denoting $t(\alpha, \beta) = x^{-\alpha}y^{-\beta}tx^\alpha y^\beta$ for $\alpha, \beta \ge 0$, the relation of $\mathcal{R}_M$ are:

1. $xy = yx$
2. $x^m r_i = r_i x^{m^2} \qquad y^m r_i = r_i y$
3. $t(a_i, b_i)r_i = r_i t(s_i, 0)$
4. $x^m l_j = l_j x \qquad y^m l_j = l_j y^{m^2}$
5. $t(a_j b_j)l_j = l_j t(0, s_j)$

where $i \in I, j \in J$.

Proposition 8 *For every modular machine $\mathcal{M}od$, it exists an Aandrea group $G(M_{\mathcal{M}od})$ associated.*

3.1.6 Valiev group

Differentrly form the previous groups, the Valiev group [14] does not depend on a monoid, Post system or a Turing or Modular machine, it can interpretate any recursively enumerable set of natural number. It'll be presented by the alphabet

$$\Sigma = \{a_i, b_i, c_i, t_i, i_{ijk}, d\}_{0 \leq i \leq m,\ 0<k<i,j<m}$$

and the relations

1. $t_0^{-1} b_0 t_0 = a_0^{-1} b_0 a_0$
2. $t_i^{-1} b_i t_i = a_i b_i c_i \qquad (1 \leq i \leq m)$
3. $t_i a_j = a_j t_i \qquad t_i c_j = c_j t_i \qquad (0 \leq i, j \leq m)$
4. $a_m d = d a_m^2 \qquad c_m d = d c_m^2 \qquad b_{m-1} d a_{m-1} b_{m-1} c_{m-1}$
5. $a_i d = d a_i (i \neq m) \qquad b d_i = d_i b (i \neq m-1) \qquad c_i d = d c_i (i \neq m)$
6. $b_i t_{ijk} = t_{ijk} a_1 b_i c_i \qquad c_i t_{ijk} = t_{ijk} t_k c_j \qquad t_{ijk} t_k = t_k t_{ijk}$
   $t_{ijk} a_s = a_s t_{ijk} (s \neq i) \qquad t_{ijk} b_s = b_s t_{ijk} (s \neq i) \qquad t_{ijk} c_s = c_s t_{ijk} (s \neq j)$

3.2 Group with standard basis

Definition 20 (Group with stable letters) *Let $\hat{G} = \langle \hat{\Sigma} | \hat{\mathcal{R}} \rangle$ be a group, the group with a system of* stable letters $\{p\}$ *and* base group $\hat{G}$ *is defined by*

$$G = \langle \Sigma = \hat{\Sigma} \cup \{p\} | \mathcal{R} = \hat{\mathcal{R}} \cup \mathcal{R}_p = \{A_i p \to pB_i\}_{i \in I} \rangle$$

where $p \notin \Sigma$ and $\forall i \in I$ $A_i, B_i \in \hat{\Sigma}^*$. A pair of corresponding *or* twin *word will be in the form*

$$\mathcal{A}_p = \mathcal{A}_{i_1}^{\pm 1}, \ldots, \mathcal{A}_{i_k}^{\pm} \qquad \mathfrak{B}_p = \mathfrak{B}_{i_1}^{\pm 1}, \ldots, \mathfrak{B}_{i_k}^{\pm}$$

thus, for $\epsilon = \pm 1$, the equality $\mathcal{A}_{p^\epsilon} p^\epsilon = p^\epsilon \mathfrak{B}_{p^\epsilon}$ where $\mathcal{A}_p^{-1} = \mathfrak{B}_p$ and $\mathfrak{B}_{p^{-1}} = \mathcal{A}_p$.

The extension system of relation *of the group G is the system of rule $\mathcal{R}_p \cup \mathcal{R}_p^{-1}$ where $\mathcal{R}_p^{-1} = \{B_i^{-1} p^{-1} \to p^{-1} A_i^{-1}$ such that $A_i p \to pB_i \in \mathcal{R}_p\}_{i \in I}$. In that system it's possible to define the* individuality of a letter*: since every transformation is in the form*

$$uwv \to uw'u \text{ with } (w = A_i p,\ w' = pB_i) \text{ or } (w = B_i^{-1} p,\ w' = p^{-1} A_i^{-1}),\ u, v \in \hat{\Sigma}^*$$

the individuality of a letter in u and v and p will be preserved.

Definition 21 (Regular system) *A system of stable letters is called* regular *if $\mathcal{A}_{p^\epsilon} \leftrightarrow^*_{\hat{\mathcal{R}}} 1 \Leftrightarrow \mathfrak{B}_{p^\epsilon} \leftrightarrow^*_{\hat{\mathcal{R}}} 1$ for any corresponding words $\mathcal{A}_p, \mathfrak{B}_p$.*

Proposition 9 *If $\{p\}$ is a regular system for $\hat{G}$, so G is an HNN-extension of $\hat{G}$.*

Demonstration: See Cor.15

Definition 22 (Insertion/cancellation) *An* insertion *is a transformation in the form $1 \to pp^{-1}$ or $\to p^{-1}p$ and its inverse it's called* cancellation

Lemma 12 *Let $Wp^\epsilon U \to W_1 p^\epsilon U_1 \to \ldots \to W_n p^\epsilon U_n$ be a chain of extended transformations, where the individuality of p^ϵ is preserved. Then there exists twin words $\mathcal{A}_{p^\epsilon}$ and $\mathfrak{B}_{p^\epsilon}$ such that*

$$W = W_n \mathcal{A}_{p^\epsilon} \qquad U = \mathfrak{B}_{p^\epsilon}^{-1} U_n$$

If there are insertion of stable letters in the chain then the words W and U can be respectively transformed into the words $W_n \mathcal{A}_{p^\epsilon}$ and $\mathfrak{B}_{p^\epsilon}^{-1} U_n$ without applying such transformations.

Demonstration: Proved by induction on the length n of the chain. For $n = 0$ is trivial. If a transformation of the chain does not apply on p^ϵ than the lemma is clear, else it is in the form $W_i \mathcal{A}_l p U_i \to W_i p \mathfrak{B}_l U_i + 1$ or $W_i \mathfrak{B}_l p^{-1} U_i \to W_i p^{-1} \mathcal{A}_l U_i$ so $W_{i+1} = W_i \mathcal{A}_{ip^\epsilon}$ and $U_{i+1} = \mathfrak{B}_{ip^\epsilon}^{-1} U_i$. Moreover in passing from the words W_i, U_i to W_{i+1}, U_{i+1} there is not insertion of stable letters.

Lemma 13 (The Novikov lemma) *Let $\{p\}$ be a regular system of stable letters and W a word in G satisfying $W = 1$. Than W can be rewrited in 1 by a chain of extended transformation, each of them is not an insertion of stable letters.*

Demonstration: Consider a step of a chain of an extended transformation $W \to \ldots \to 1$ in which there is an insertion of the letter p:

$$W \to \ldots \to W_{i-1} = VV' \to W_i = Vp^\epsilon p^{-\epsilon}V' \to \ldots \to 1$$

since the letters $p\epsilon$ and $p^{-\epsilon}$ should be cancelled during the transformation, there are two cases:

- the cancellation involves only the this two letters:

  $$W \to \ldots \to W_i = V_1 p^\epsilon p^{-\epsilon} V_1' \to \ldots \to V_k p^\epsilon p^{-\epsilon} V_k' \to V_k V_k' = W_k \to \ldots \to 1$$

  so by the Lemma 12 there exist twin words $\mathcal{A}_{1p^\epsilon}, \mathcal{A}_{2p^\epsilon}\mathfrak{B}_{1p^\epsilon}, \mathfrak{B}_{2p^\epsilon}$ such that the words $V_1, 1, V_1'$ can be transformed into the words $V_k\mathcal{A}_{1p^\epsilon}, \mathfrak{B}_{1p^\epsilon}^{-1}\mathfrak{B}_{2p^\epsilon}$ and $\mathcal{A}_{2p^\epsilon}^{-1}V_k'$ without insertion of stable letters. Since $\{p\}$ is regular in G holds $\mathfrak{B}_{1p^\epsilon}^{-1}\mathfrak{B}_{2p^\epsilon} = 1$ iff $\mathcal{A}_{1p^\epsilon}\mathcal{A}_{2p^\epsilon}^{-1} = 1$. So W_i can be transformed in W_k without insertion of stable letters, then is possible to obtain the same transformation eliminating this insertion of stable letters.

- else the chain is in the form:

  $$W \to \ldots \to W_i = V_1 p^\epsilon V_1' p^{-\epsilon} p^\epsilon V_1'' \to \ldots$$

  $$\ldots \to V_k p^\epsilon p^{-\epsilon} V_k' p^\epsilon V_k'' \to V_k V_k' p^\epsilon V_k'' = W_k \to \ldots \to 1$$

  by lemma 12 there exists pairs of twin words $\mathcal{A}_{ip^\epsilon}, \mathfrak{B}_{ip^\epsilon}, i = 1,2,3$ such that the words $V_1, V_1', 1$ and V_1'' can be transformed respectively in $V_k\mathcal{A}_{1p^\epsilon}$, $\mathfrak{B}_{1p^\epsilon}^{-1}\mathcal{A}_{2p^{-\epsilon}}$, $\mathfrak{B}_{2p^{-\epsilon}}^{-1}V_k'\mathcal{A}_{3p^\epsilon}$ and $\mathfrak{B}_{3p^\epsilon}^{-1}V_k''$, hence the word W_i can be transformed into

  $$V_k\mathcal{A}_{1p^\epsilon}p^\epsilon\mathfrak{B}_{1p^\epsilon}^{-1}\mathcal{A}_{2p^{-\epsilon}}\mathfrak{B}_{3p^\epsilon}^{-1}V_k''$$

  and applying the transformations in the extended system W_i become

  $$V_k\mathcal{A}_{1p^\epsilon}\mathcal{A}_{1p^\epsilon}^{-1}\mathcal{A}_{2p^\epsilon}\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k''$$

  which can be transformed in

  $$V_k\mathcal{A}_{2p^\epsilon}\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k'' = V_k\mathfrak{B}_{2p^{-\epsilon}}\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k''$$

  and by the insertion of $1 = \mathfrak{B}_{2p^{-\epsilon}}^{-1}V_k'\mathcal{A}_{3p^\epsilon}$ (which doesn't contain stable letters)

  $$V_k\mathfrak{B}_{2p^{-\epsilon}}\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k'' \to V_k\mathfrak{B}_{2p^{-\epsilon}}1\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k'' \to$$

  $$\to V_k\mathfrak{B}_{2p^{-\epsilon}}\mathfrak{B}_{2p^{-\epsilon}}^{-1}V_k'\mathcal{A}_{3p^\epsilon}\mathcal{A}_{3p^\epsilon}^{-1}p^\epsilon V_k'' \to^2 V_k V_k' p^\epsilon V_k'' = W_k$$

  again is possible to decrease the number of insertions in the chain.

the lemma follows by induction on the number of insertion in the chain.

Lemma 14 (The Britton's lemma) *Let $\{p\}$ be a regular system of stable letters for the group G over $\hat{G}$ and W a word in G such that $W = 1$ in G. Than W is a word in $\hat{G}$ and $W =_{\hat{G}} 1$ or W includes the subword $p^{-\epsilon}Ap^\epsilon$ where $A \in \hat{G}$ and $A =_{\hat{G}} \mathcal{A}_{p^\epsilon}$.*

Demonstration: By Novikov's lemma, the word W can be transformed in 1 without insertion of stable letters, so if the chain

$$W \to W_1 \to \ldots \to W_n = 1$$

contain no stable letters then $W \in \hat{G}$ and $W =_{\hat{G}} 1$. If W contains the letter p, then it should be cancelled during the transformation. Considering the first cancellation of a stable letters occurring in the chain

$$W = Vp^{-\epsilon}V'p^{\epsilon}V'' \to \ldots \to W_k = V_k p^{-\epsilon}p^{\epsilon}V'_k \to V_k V'_k = W_{k+1}$$

where V' does not contain the stable letters. By lemma 12 there exists a pairs of twin words $\mathcal{A}_{ip^{\epsilon}}, \mathfrak{B}_{ip^{\epsilon}}, i = 1, 2$ such that the words V, V', V'' can be transformed into the words $V_k\mathcal{A}_{1p^{-\epsilon}}, \mathfrak{B}^{-1}_{1p^{-\epsilon}}\mathcal{A}_{2p^{\epsilon}}$ and $\mathfrak{B}^{-1}_{2p^{\epsilon}}V'_k$ without insertion of stable letters. Hence $V' \in \hat{G}$ since $V' = \mathfrak{B}^{-1}_{1p^{-\epsilon}}\mathcal{A}_{2p^{\epsilon}} = \mathcal{A}{-1}_{1p^{\epsilon}}\mathcal{A}_{2p^{\epsilon}} = \mathcal{A}_{p^{\epsilon}}$

Corollary 15 *If $\{p\}$ is a regular system of stable letters of the group G over $\hat{G}$ than $\hat{G} < G$.*

Definition 23 *A word W of a group with stable letters $\{p\}$ is called p-reducible if W includes a subword in the form $p^{-\epsilon}Ap^{\epsilon}$ where $A \in \hat{G}$ and $A =_{\hat{G}} A_{p^{\epsilon}}$*

With this definition is possible to reformulate the Britton's lemma: if $W =_G 1$ and W contains stable letters, so for some stable letters W is p-reducible.

Introducted by Bokut' in [2] a *standard basis* or *standard normal form* permits to have a canonical form to write an element of a Novikov-Boone group given one of its presentation.

3.2.1 The definition of groups with standard normal form

Let's consider a sequence of HNN-extension $G_0, G_i, \ldots, G_n$ where G_0 is a free group and the group G_{i+1} is obtained adjoining to the group G_i letters $\{p\}$ and defining relation

$$A_l p = pB_l$$

where $p \in \{p\}$ it's called letter of *weight* $i+1$ and $A_l, B_l \in G_i$ contain exactly one letter of the highest weight. So in the group G_{i+1} an arbitrary relation can be represented in the form

$$A'xA''p = pB'yB''$$

where x and y are the letters of highest weight (if the power of these letters are different from ± 1 will be considered its first or last occurrence). For every relation will be associated four types of *prohibited words*:

$$x\mathfrak{B}_x A''p \qquad x^{-1}\mathfrak{B}_{x^{-1}}A'^{-1}p \qquad y\mathfrak{B}_y B''p^{-1} \qquad y^{-1}\mathfrak{B}_{y^{-1}}B'^{-1}p^{-1}$$

Is so possible to define by induction on i the notion of *canonical word*: every reduced word of G_0 are in canonical form, an irreducible word

$$U = U_1 p^{\epsilon_1} U_2 p^{\epsilon_2} \ldots U_k p^{\epsilon_k} U_{k+1}$$

in the group G_{i+1} where $U_j \in \hat{G}$ and p_j are letters of weight $i+1$ $k \geq 0$ is canonical if, for every j:

- U_j are canonical words in the group G_i
- U doesn't include subword of an any prohibited types in G_{i+1}

Is so possible to reduce a word $U = U_1 p^\epsilon U_2 \dots U_{n-1} p^\epsilon U_n$ in canonical $C(U)$ by the following algorithmic process:

1. reduce every word U_j to canonical form in the group G_i
2. perform all possible cancellation of letters of weight $i+1$
3. eliminate the first occurrence (from the right) of a prohibited word following the following role[3]

$$x\mathfrak{B}_x A''p \to \mathcal{A}_x A'^{-1} pB \qquad x^{-1}\mathfrak{B}_{x^{-1}} A'^{-1}p \to \mathfrak{B}_x A''pB^{-1}$$

$$y\mathfrak{B}_y B''p^{-1} \to \mathcal{A}_y^{-1} B'^{-1} p^{-1} A \qquad y^{-1}\mathfrak{B}_{y^{-1}} B'^{-1} p^{-1} \to \mathfrak{B}_y B'' p^{-1} A^{-1}$$

   where $\mathcal{A}_z$ and B_z (with $z = x$ or y) are twin words.

4. return to step 1

Definition 24 *The group G_{i+1} is called group with* standard normal form *or group with* standard basis *if every word U can be reduced to canonical form $C(U)$ in a finite number of steps*[4]*. If that condition it's satisfy for every i the group G is a group with standard normal form.*

Lemma 16 *Let G_i a group with standard normal form then the canonical for of an arbitrary word of the group G_{i+1} is unique iff the following condition are met:*

- *p is a system of stable letters*
- *If the word Up^ϵ and Vp^ϵ are canonical $U, V \in G_i$, p letter of weight $i+1$ and $U = V\mathcal{A}_{p^\epsilon}$ then the equality $\mathcal{A}_{p^\epsilon} =_{G_i} 1$ holds*

Lemma 17 *Let G_i be a group with standard normal form and $\{p\}$ a regular system of stable letters. Suppose that any word $\mathcal{A}_{p^\epsilon} \neq_{G_i} 1$ with the letter p of weight $i+1$ is representable as*

$$\mathcal{A}_{p^\epsilon} =_{G_i} V_1 x_1 V_2 x_2 V_3$$

where x_1, x_2 are letters of highest weight and the word is x-irriductible for every letter x of higher weight. If an arbitrary word of the form

$$x_2 C(\mathfrak{B} x_2 V_3) p^\epsilon \qquad x_1^{-1} C(\mathfrak{B} x_1^{-1} V_1^{-1}) p^\epsilon$$

is prohibited or includes a prohibited subword (with respect to the letter p) then the second condition of Lemma 16 are satisfied.

[3]Every of these role derive by the relation $A'\mathcal{A}_x x\mathfrak{B}_x A''p = pB'\mathcal{A}_y y\mathfrak{B}_y B''$, where $B = B'yB'', A = A'xA''$ and

[4]see **??**

Chapter 4

Undecidibility of the word problem for the groups

4.1 Novikov-Boone's demonstration

In [2] Bokut represent the proofs of Novikov-Boone's theorem proving that Novikov's group $\mathfrak{A}_{p_1p_2}$ and Boone's groups $G(T,q)$ has standard basis. It make it easyer (Cap.4.1 or Bokut [3]) to prove that exist a finitely presented group in which conjugacy problem ($\mathfrak{A}_{p_1p_2}$)is unsolvable and the word problem for the group $G(T,q)$ can have any fixed Turing degree of unsolvability.

4.1.1 The Boone group

To introduce the Boone group $G(T,q)$ is needed to extend the concept of stable letters to system with more than one letter. A set $P = \{p_m\}$ is a system of stable letters of a group G over $\hat{G}$ if the group G can be presented by

$$G = \langle \Sigma_{\hat{G}} \cup \{p_m\} | \mathcal{R}_{\hat{G}} \cup \{A_i p_{m_i} = p_{n_i} B_i | A_i, B_i \in \hat{G}\}\rangle$$

The letters involved in the same relation are called *contiguous.* Completing this definition with transitivity and reflexivity is obtained a partition of P given by $\bigcup_{n\in I}\{p_m\}_{m\in P_n}$ where all the $p_m \in P_n$ are contiguous to a fixed p_n for every $n \in I$. Since exist A'_{n_i}, B'_{n_i} such that $A_{n_i}p_{n_i} = p_n B'_{n_i}$ so by $p_{n_i} = A'^{-1}_{n_i} p_n B'_{n_i}$ is possible to eliminate all the p_m with $m \notin I$ and so present the group in the form

$$G = \langle \Sigma_{\hat{G}} \cup \{p_m\}_{m\in I} | A'_{n_l} p_n = p_n F_{n_l}\rangle$$

Definition 25 *The system P of stable letters is* regular *if every $p_m \in I$ are stable letters. For p_{n_i}, p_{n_j} contiguous is possible to define*

$$\mathcal{A}_{p_{n_i},p_{n_j}} = A'_{n_j}\mathcal{A}_{p_n}A'_{n_i} \qquad \mathfrak{B}_{p_{n_i},p_{n_j}} = B'_{n_j}\mathfrak{B}_{p_n}B'_{n_i}$$

where $A'_{n_j}, A'_{n_i}, B'_{n_j}$ and B'_{n_i} are words participating in the relation which links letters p_{n_i}, p_{n_j} to p_n. It is also valid the following notational equality

$$\mathcal{A}_{p^{\epsilon}_{n_i}p^{\epsilon}_{n_i}} = \mathfrak{B}_{p^{-\epsilon}_{n_j}p^{-\epsilon}_{n_i}}$$

In the same manner of Chap. 3.2 is possible to define the individuality of a letter and extended system of transformation to reformulate the lemmas 12, Britton's and Novikov's lemmas. For example the analogous of lemma 12 tell that, given a chain of extended transformation

$$Wp^{\epsilon}_{n_1}U \to W_1 p^{\epsilon} U_1 \to \ldots \to W_k p^{\epsilon}_{n_k} U_k$$

where $p^{\epsilon}_{n_i}$ have the same individuality. Then there exists twin words $\mathcal{A}_{p^{\epsilon}_{n_i} p^{\epsilon}_{n_i}}$ and $\mathfrak{B}_{p^{\epsilon}_{n_i} p^{\epsilon}_{n_i}}$ such that

$$W = W_n \mathcal{A}_{p^{\epsilon}_{n_k} p^{\epsilon}_{n_1}} \qquad U = \mathfrak{B}^{-1}_{p^{\epsilon}_{n_1} p^{\epsilon}_{n_k}} U_n$$

while Britton lemma tells that given a regular system of stable letters P of a group G over $\hat{G}$ and a word $W =_G 1$ than either $W \in \hat{G}$ and $W =_{\hat{G}} 1$ or W includes subword of the form $p^{-\epsilon}_{n_j} \mathcal{A}_{p^{\epsilon}_{n_i} p^{\epsilon}_{n_j}} p^{\epsilon}_{n_i}$.

Let's now build the Boone group like a succession of HNN extension, for every extension will be given them additional generators and relations, the letters of maximal weight that will appear in the definition of prohibiten words will be highlited and there will be explicitated the twin words form.

Definition 26 (Boone group) *Let T be a* special *semigroup, i.e. a semgroup generated by $\{s_d, q_e\}_{d \in D, e \in E}$ and relations $A_i = B_i, 1 \le i \le N$ where A_i, B_i* special words *($A_i, B_i = Sq_eS'$ where S, S' are $\{s_d\}$-words).*

- $G_0 = \langle x, y \rangle$
- G_1*:* $\{s_d | d \in D\} \quad | \quad \mathbf{y} y s_d = s_d \mathbf{y},\ \mathbf{x} s_d = s_d x \mathbf{x}$
  $\mathcal{A}_{s_d} = V(x, y^2) \qquad \mathfrak{B}_{s_d} = V(x^2, y)$
- G_2*:* $\{l_i, r_i | 1 \le i \le N\} \quad | \quad \mathbf{s_d} l_i = y l_i y \mathbf{s_d},\ \mathbf{s_d} x r_i x = r_i \mathbf{s_d}$
  $\mathcal{A}_{l_i} = V(y^{-1}s_d), \mathfrak{B} = V(ys_d), \mathcal{A}_{r_i} = V(s_d x), \mathfrak{B}_{r_i} = V(s_d x^{-1})$
- G_3*:* $\{q_e | e \in E\} \quad | \quad A_i = \mathbf{l_i} B_i \mathbf{r_i}, A_i = A'_i q_{n_i} A''_i, B_i = B'_i q_{m_i} B''_i$
  A'_i, A''_i, B'_i, B''_i *$\{s_b\}$-words*
  $\mathcal{A}_{q_{m_i} q n_i} = V(A'^{-1}_i l_i B'_i), \mathfrak{B}_{q_{n_i} p_{m_i}} = V(A''_i r^{-1}_i B''^{-1}_i)$
- G_4*:* $\{t\} \quad | \quad \mathbf{l_i} t = t \mathbf{l_i},\ \mathbf{y} t = t \mathbf{y}$
  $\mathcal{A}_t = V(l_i, y) = \mathfrak{B}_t$
- *fixed a* $q \in \{q_e\}$, G_5*:* $\{k\} \mid \mathbf{r_i} k = k \mathbf{r_i},\ \mathbf{x} k = k \mathbf{x}, q^{-1} \mathbf{t} q k = k q^{-1} \mathbf{t} q$
  $\mathcal{A}_k = V(r_i, x, q^{-1}tq) = \mathfrak{B}_k$

Theorem 18 *The Boone group $G(T, q) = G_5$ have a standard basis.*

Demonstration: Let's build the set C_i of the words in standard normal form for every G_i

- C_0 is equal to the set of all irreducible words on the alphabet $\{x, y\}$ (also negative letters), by definition $\mathcal{A}_x = \mathfrak{B}_x = \mathcal{A}_y = \mathfrak{B}_y = 1$
- the set C_1 it's constituited by words in the form

$$C(W) = U_1 s_{d_1} U_2 \ldots U_k s_{d_k} U_{k+1}$$

where $U_i \in C_0$ and $C(W)$ does not contain subword in the form

$$\alpha\mathfrak{B}_\alpha A''p \qquad \alpha^{-1}\mathfrak{B}_{\alpha^{-1}}A'^{-1}p \qquad \beta\mathfrak{B}_\beta B''p^{-1} \qquad \beta^{-1}\mathfrak{B}_{\beta^{-1}}B'^{-1}p^{-1}$$

so, since $A = \mathbf{y}y, B = \mathbf{y}$ $(A' = 1, A'' = yB' = B'' = 1)$ or $A = \mathbf{x}, B = x\mathbf{x}$ $(A' = A'' = 1, B' = x, B'' = 1)$, the prohibiten words wil be in the form:

$$yV(y)A''s_d \qquad y^{-1}V(y)A'^{-1}s_d \qquad yV(y)B''s_d^{-1} \qquad y^{-1}V(y)B'^{-1}s_d^{-1}$$

$$xV(x)A''s_d \qquad x^{-1}V(x)A'^{-1}s_d \qquad xV(x)B''s_d^{-1} \qquad x^{-1}V(x)B'^{-1}s_d^{-1}$$

so them have to contain a subword in the form:

$$y^2s_d \qquad y^{-1}s_d \qquad ys_d^{-1} \qquad y^{-2}s_d^{-1}$$

$$xs_d \qquad x^{-1}s_d \qquad xs_d^{-1} \qquad x^{-2}s_d$$

so in that simple case is possible to see that in a normal form word in G_1 before a positive s_d there could be:

1. the word before a positive s_d have to terminate with a single occurrence of an y
2. the word before a negative s_d have to terminate with a single occurrence of a negative x

- the set C_2 it's consists of reduced word in the form

  $$U_1\alpha_{i_1}U_2\dots U_k\alpha_{i_k}U_{k+1}$$

  where $U_i \in C_1$, $\alpha_{i_j} \in \{r_i, l_i | i \leq i \leq N\}$ containing no subword in the form:

  $$s_dV(x^2,y)l_i^\epsilon \qquad s_d^{-1}V(x,y^2)y^\epsilon l_i^\epsilon$$
  $$s_dV(x^2,y)x^\epsilon r_i^\epsilon \qquad s_d^{-1}V(x,y^2)r^\epsilon$$

  where V, Vx^ϵ ,Vy^ϵ (where$V = V(x^2,y)$ or $V(x,y^2)$) are reduced, $d \in D$, $1 \leq i \leq N$. Since a word $\mathcal{A}_l$ can be in the form ySy^{-1} with S reduced word in $\{s_d\}$, elimination rule could not and the word in the form

  $$s_dV(x^2,y)l_i^\epsilon \qquad s_d^{-1}V(x,y^2)y^\epsilon l_i^\epsilon$$

  are prohibited, lemma 17 is verified for that kind of word (choosing x_1 the first letter of S and x_2 the last one), else lemma 16 holds.

- To verify the existence of the standard basis will suffice to use the lemma 16 G_3: since a word $\mathcal{A}_{q_mq_n}, \mathfrak{B}_{q_mq_n}$ are equal to 1 iff his projection on the alphabet $\{l_i, r_i\}$ is equal to 1. It follows that the letters q_e are regoular and as above is possible to apply the lemma 17, so G_3 is a gruop with standard basis.

- In G_4 the prohibited word are in the form

  $$y^\delta t^\epsilon \qquad l_iC(y^{-1}SyV(y))t^\epsilon \qquad l_i^{-1}C(ySy^{-1}V(y))t^\epsilon$$

  where $\delta = \pm1$ and S a reduced $\{s_d\}$-word. Since every elimination of prohibited word reduce the number of l_i or y. The lemma 16 is proved because if two reduced word Ut, Wt where $U = W\mathcal{A}_t = WV(l_i,y)$ than $V(l_i,y) = 1$.

- Finally a normal form word contains no subword of form

$$r_i^\delta k^\epsilon \qquad x^\delta k^\epsilon \qquad t^\delta C(V(l_i,y)qW(r_i,x))k^\epsilon$$

where $\delta = \pm 1$. The presence of $W(r_i, x)$ in the last class of prohibited word is due to the fact that $W(r_i, x)$ commute with k and by the fact that, if Σ is a special word of T such that $\Sigma =_T q$, then $\Sigma^{-1}t\Sigma k =_{G_5} k\Sigma^{-1}t\Sigma$

Lemma 19 *The word problem for the gour G_4 is solvable*

Lemma 20 *Let S, S' special word in T then $S =_T S'$ iff*

$$S =_{G_3} V(l_i,y)S'W(r_i,x)$$

Lemma 21 *The problem for a word U of the group G_3 to wqual to a word in the form $V(l_i,y)SW(r_i,x)$ with S a special word is solvable*

Theorem 22 *The Turing degree of unsolvability of the word problem for the group $G(T,q)$ coincides with the Turing degree of the problem to a special word of T to equal the word q.*

Demonstration: By lemma 19 and Theor.18 is possible, for all word $W \in G$, to calculate its normal form $C(W) = U_1kU_2k \dots U_nkU_{n+1}$ in a finite number of reduction. Since the word problem of G_4 is solvable the problem is deduced determinate if a word Q in G_3 is equal or not to a word $V(l_i,y)qW(x,r_i)$. By lemma 21 is possible to determinate if a word Q is equal to a word in the form $V(l_i,y)\Sigma W(x,r_i)$. So lemma 16 the decidability of word problem for $G(T,q)$ can be reduced to decidability to equivalence problem for the monoid T.

Corollary 23 (Undecidability of word problem for the groups) *There exists a finitely presented gruop with undecidable word problem*

Demonstration: By Theo.26 exists a finite presented monoid T with defining relation given by special words and undecidable word problem, so by Theo.22 the associated Boone group will have undecidable word problem.

4.2 Aandreaa and Cohen's demonstration

Using the affine machines it's possible to give a more intuitive demonstration of the theorem like given in [1] by Cohen Aandrea and in a simplify way by Lafont in [9]. Here will be used the same notation of Theor.3 : $F_2 = \langle a, b\rangle$ and $a_n = b^n a b^{-n}$

Lemma 24 *For all $p, p', q, q', z \in \mathbb{Z}$, $q, q' \neq 0$ exist an isomorphism $\phi : F_2 \to F_2$ such that $\phi(a_{p+qz}) = a_{p'+q'z}$*

Demonstration: By Lem. 4 $\langle a_p, b^q\rangle = F_2 = \langle a_{p'}, b^{q'}\rangle$ so exist an isomorphism ϕ such that $\phi(a_p) = a_{p'}$ and $\phi(b^q) = b^{q'}$ and so

$$\phi(a_{p+qz}) = \phi((b^q)^z a_p (b^{-q})^z) = \phi((b^q)^z)\phi(a_p)\phi((b^{-q})^z) = (b^{q'})^z a_{p'} (b^{-q'})^z = a_{p'+zq'}$$

Notation: Let $I \subset \mathbb{Z}$, $[P]_{F_2}$ is the su bset of F_2 generated by the set $\{a_z | z \in \mathbb{Z}\}$

Lemma 25 *Let $p, q \in \mathbb{Z}$, so $\langle a_p, b^q \rangle \cap [\mathbb{Z}]_{F_2} = [p + q\mathbb{Z}]_{F_2}$*

Demonstration: Let $K = [p + q\mathbb{Z}]_{F_2}$. Every reduced word w in $\langle a_p, b^q \rangle$ can be written in the form uv with $u \in K$ and $v \in \langle b^q \rangle$, because there are $k_i \in \mathbb{Z}$ and $\delta_i \in \{-1, 1\}$ such that

$$w = b^{k_0 q} a_{\delta_1 p} b^{k_1 q} a_{\delta_2 p} \cdots a_{\delta_n p} b^{k_n q} =$$

$$= b^{m_0 = k_0 q + \delta_1 p} a b^{m_1 = k_1 q + (\delta_2 - \delta_1) p} a \cdots a b^{m_n = k_n q - \delta_n p} =$$

$$= a_{m_0} a_{m_1 + m_0} \cdots a_{\Sigma_{i=0}^{j} m_i} \cdots a_{\Sigma_{i=0}^{n-1} m_i} b^{\Sigma_{i=1}^{n} m_i}$$

Let $\pi : F_2 \to \langle b \rangle$ the projection of F_2 on $\langle b \rangle$ (i.e. $\pi(a) = 1, \pi(b) = b$), so $K \subseteq [\mathbb{Z}]_{F_2} \subseteq ker(\pi)$ and $\forall x \in \langle a_p, b_q \rangle, \pi(x) = \pi(uv) = \pi(u)\pi(v) = \pi(v) = v$ so $[\mathbb{Z}]_{F_2} \cap \langle a_p, b^q \rangle \subseteq K$. By $K \subseteq [\mathbb{Z}]_{F_2}$ and $k \subseteq \langle a_p, b_q \rangle$ follows the equality.

Demonstration: [Undecidability of word problem for the groups] Let $m \in \mathbb{Z}$ and $\mathcal{A}$ machine affine. It's possible to associate for every transition of $\mathcal{A}$ a local isomorphism ϕ_i. By the Theor.11 is possible to obtain an extension of $F_{\mathcal{A}}$ of F_2 with stable letters $t_1 \ldots t_n$ which represents the local isomorphism $\phi_1 \ldots \phi_n$. Let $P = \{z \in \mathbb{Z} | z \leftrightarrow^*_{\mathcal{A}} m\}$ and $H = \langle a_m, t_1, \ldots t_n \rangle$. By Lemma 24 follow:

- if $z \to_{\mathcal{A}} z'$ so $a_{z'} = \phi_i(a_z) = t_i a_z t_i^{-1}$ exist an $i \in \{1, \ldots, n\}$
- if $z \leftrightarrow^*_{\mathcal{A}} z'$ so $a_{z'} = \phi_{i_n} \circ \ldots \circ \phi_{i_1}(a_z) = u a_z u^{-1}$ exist an $u \in \langle t_1, \ldots t_n \rangle$

so $K \subseteq H$ because $a_m \in K$ and for every $z \leftrightarrow^*_{\mathcal{A}} m$, $a_m \leftrightarrow^*_{\mathcal{A}} a_z$ and $K = K \cap [\mathbb{Z}]_{F_2} = H \cap [\mathbb{Z}]_{F_2}$. Moreover K it's invariant for every local isomorphism ϕ_i because

$$\langle a_p, b^q \rangle \cap K = \langle a_p, b^q \rangle \cap [\mathbb{Z}]_{F_2} \cap K = [p + q\mathbb{Z}]_{F_2} \cap [P]_{F_2} = [(p + q\mathbb{Z}) \cap P]_{F_2}$$

and so (see Theo. 11) $K = H \cap F_2$.
So is possible to see that exists an extension $F_{\mathcal{A}}$ finitely presented of F_2 and $u \in F$ such that

$$a_z u = u a_m \text{ in } F_{\mathcal{A}} \Leftrightarrow a_z \in H \Leftrightarrow a_z \in K = [P]_{F_2} \Leftrightarrow z \leftrightarrow^*_{\mathcal{A}} m$$

Therefore the word problem for group $F_{\mathcal{A}}$ is reducible to the $\mathcal{H}alt$ problem for the machine affine $\mathcal{A}$ which can be chose with any Turing degree of unsolvability (see Prop.**??**).

Appendix A

Combinatorial system

Rewriting system, Post system, Thue system are different system of substitution of substrings in strings with the same base concept:

Definition 27 (production) *Fixed an alphabet* Σ*, a* rewrite rule*,* semi-Thue production*or simply* production *is an expression*

$$u \to v$$

if P *is a semi-Thue production* $u \to v$*,* $A, B \in \Sigma^*$

$$A \to_P B$$

mean that exists $A', A'', B', B'' \in \Sigma^*$ *such that* $A = A'uA''$ *and* $B = B'vB''$ *A* normal production *is a produictin in the form* $uv \to vu'$*. Two word in* $u, w \in \Sigma^*$*.*

Definition 28 *A* combinatorial system *consists of an alphabet and a set of pair of words callad production.*

A semi-Thue system *or* string rewrite system $S = (\Sigma|\mathcal{R})$ *is given by an alphabet and a finite set of rewriting rule. A* Thue system *is a semi-Thue system where for every rewriting role* $u \to v$ *exists its inverse* $v \to u$*. A* Post system $P = [\Sigma; \Phi]$ *is a combinatorial system with a finite set of normal production. Two word are called* equivalent *in* P *(written* $u \sim_P w$ *) if there exists a sequence of normal production which transform* u *in* w*.*

Proposition 10 *Every non deterministic Turing machine can be simulated by a semi-Thue system*

Demonstration: Let Σ the alphabet and $Q = \{q_i\}$ the states of T. Is so possible to write the tape of the Turing macine as a special word of $\Sigma \cup Q$ where the letters q_i corresponding to the state for turing machine is positionated before the letter read by the head. Is so possible to code the computing of T as a string rewriting system ([8]).

Theorem 26 (Post-Markov ([13],[11]) *Exists a finite semigroup with undecidable word problem.*
More precisely it exists a monoid finitely presented with rewriting rule expressed by special words.

Corollary 27 *The following example is given by Ceitin in [7]*

Theorem 28 *The semigroup $\langle a, b, c, d | \mathcal{R} \rangle^+$ where $\mathcal{R}$ are the relations*

$$ac = ca \qquad ad = da \qquad bd = db \qquad ce = eca \qquad dc = edb \qquad cca = ccae$$

has unsolvable word problem.

Bibliography

[1] *S. Aandreaa & E. Cohen,* Modular machines, the word problem for finitely presented groups, Collins' theorem*, Word Problems II. (1980) p.1-16*

[2] *L.A. Bokut',* Groups with a relative standard basis*, Sibirskii matematichan Z. 9, N.3 (1968) p.4-52, 1980, p.29-53*

[3] *L.A.Bokut',* The degrees of unsolvability for the conjugacy problem for finitely presented groups*, Algebra and Logic7 , N.5 (1968) p.4-70, N.6 (1968) p.4-52*

[4] *L.A. Bokut',* Malcev's problem and groups with a normal form*, Word Problems II (1980) p.29-53*

[5] *L.A. Bokut',* Algorithmic and Combinatorial Algebra*, Kluwer Academic Publisher (1994), chap.6-7*

[6] *W.W. Boone* The word problem*, Annals of mathematics (1959), vol.70, N.2, p.207-265*

[7] *G.S.Ceitin,* Associative calculus with undecidable equivalence problem*, Dokl. Akad. Nauk SSSR (1956), vol.107, N. 3 , p.370-371(in russian)*

[8] *M.D.Davis and E.J.Weyuker,* Computability, complexity and lenguages*, Accademic Press (1983), p.118-146*

[9] *Y.Lafont,* Réécriture et problem du mot*, Gazette des mathématiciens 120 (2009) p.27-38*

[10] *M.L.Minsky,* Recursive unsolvability of Post problem of "Tag" and other topics in theory of Turing machines *, Annals of math. (1961), Vol.74,N.3, p.437-455*

[11] *A.A.Markov,* On the impossibility of certain algorithm in the theory of associative systems*, Dokl. Akad. Nauk SSSR (1947), vol.55, p.587-590(in russian)*

[12] *P.S. Novikov* On algorithmic undecidability of the word problem*, Dokl. Akad. Nauk SSSR (1952), vol.85, N.4, p.485-524 (in russian)*

[13] *E.L. Post,* Recursive unsolvability of a problem o Thue*, The journal of sybolic logic(1947), vol.12, p.1-11*

[14] *M.K.Veliev ',* On a problem of G. Higman*, Algebra i logika, 1968, Vol7, N.3, O.9-22 (in russian)*