# Independent Sets in Free Groups and Fields

Rev. Charles McCoy & Russell Miller

Univ. of Portland

Queens College / CUNY Graduate Center

Rutgers Logic Seminar
18 February 2013

# Computable Groups

## Definitions

A *presentation* of a countable group $G$ is simply a group isomorphic to $G$, whose domain is $\omega$. (That is, the elements are natural numbers – or at least, are indexed by natural numbers.)
A presentation of $G$ is *computable* if the group operation $\cdot$ for $G$ is a Turing-computable function: $\omega \times \omega \to \omega$.

Thus, in a computable group, we can compute the product $x \cdot y$ of any given pair $(x, y) \in \omega^2$ of elements. Since the domain is $\omega$, we can effectively find the identity element $e \in \omega$ of $G$: this $e$ is unique in satisfying $e \cdot e = e$. We can also compute the inversion function on $G$: given $x \in \omega$, just search for some $y \in \omega$ such that $x \cdot y = e$.

# Computable Groups

## Definitions

A *presentation* of a countable group $G$ is simply a group isomorphic to $G$, whose domain is $\omega$. (That is, the elements are natural numbers – or at least, are indexed by natural numbers.)
A presentation of $G$ is *computable* if the group operation $\cdot$ for $G$ is a Turing-computable function: $\omega \times \omega \to \omega$.

Thus, in a computable group, we can compute the product $x \cdot y$ of any given pair $(x, y) \in \omega^2$ of elements. Since the domain is $\omega$, we can effectively find the identity element $e \in \omega$ of $G$: this $e$ is unique in satisfying $e \cdot e = e$. We can also compute the inversion function on $G$: given $x \in \omega$, just search for some $y \in \omega$ such that $x \cdot y = e$.

It is not so clear, however, whether we can decide if an arbitrary $x \in G$ lies in $G^2 = \{y \cdot y \ : \ y \in G\}$, or other questions involving quantifiers.

# A first example

The free divisible abelian group on countably many generators is often viewed as a vector space over $\mathbb{Q}$, of dimension $\omega$. With an effective listing $\{q_0, q_1, \ldots\}$ of $\mathbb{Q}$, we can readily list out the set $V_\omega$ of all finite tuples $(q_{i_1}, \ldots, q_{i_n}) \in \mathbb{Q}^{<\omega}$ with $q_{i_n} \neq 0$. Treating such a tuple as $(q_{i_1}, \ldots, q_{i_n}, 0, 0, \ldots)$ makes $V_\omega$ a computable presentation of this group, under componentwise addition.

# A first example

The free divisible abelian group on countably many generators is often viewed as a vector space over $\mathbb{Q}$, of dimension $\omega$. With an effective listing $\{q_0, q_1, \ldots\}$ of $\mathbb{Q}$, we can readily list out the set $V_\omega$ of all finite tuples $(q_{i_1}, \ldots, q_{i_n}) \in \mathbb{Q}^{<\omega}$ with $q_{i_n} \neq 0$. Treating such a tuple as $(q_{i_1}, \ldots, q_{i_n}, 0, 0, \ldots)$ makes $V_\omega$ a computable presentation of this group, under componentwise addition.

Moreover, in this presentation $V_\omega$, there is a computable basis $B_0$, namely $\{(0, \ldots, 0, 1) \in \mathbb{Q}^{n+1} : n \in \omega\}$.

Indeed, for every set $S \subseteq \omega$, we also have a basis $B_S \equiv_T S$:

$$B_S = \{(0, \ldots, 0, 1) \in \mathbb{Q}^{n+1} : n \notin S\} \cup \{(0, \ldots, 0, 2) \in \mathbb{Q}^{n+1} : n \in S\}.$$

# Complications

There are other computable presentations of the free divisible abelian group in which no basis is computable. We now describe one:

Start building $U$ just like $V_\omega$ above, one element at a time. Simultaneously enumerate all c.e. sets $W_e$. When/if any $W_{e,s}$ has enumerated $2e+2$ elements, check whether $W_{e,s}$ is linearly independent in the group $U_s$ built so far. If not, then keep going. If so, then (dropping the current identification with $\mathbb{Q}^{<\omega}$) we decree that in $U_{s+1}$, one of these elements is a large rational multiple of another one.

# Complications

There are other computable presentations of the free divisible abelian group in which no basis is computable. We now describe one:

Start building $U$ just like $V_\omega$ above, one element at a time. Simultaneously enumerate all c.e. sets $W_e$. When/if any $W_{e,s}$ has enumerated $2e + 2$ elements, check whether $W_{e,s}$ is linearly independent in the group $U_s$ built so far. If not, then keep going. If so, then (dropping the current identification with $\mathbb{Q}^{<\omega}$) we decree that in $U_{s+1}$, one of these elements is a large rational multiple of another one.

Doing this forever gives a computable presentation $U$ of a group which is still abelian, divisible, and free of dimension $\omega$, yet no infinite c.e. set $W_e$ can be linearly independent in $U$. So $U$ has no c.e. basis, let alone any computable basis.

(Fact: in a computable free structure, all c.e. bases are computable.)

# A reasonable resolution

## Proposition

Every computable presentation $U$ of the free divisible abelian group $\mathbb{Q}^{<\omega}$ has a $\Pi^0_1$ basis, which may be taken to be of the same Turing degree as the *dependence relation* on $U$:

$$D_U = \{(x_1, \ldots, x_n) \in U^{<\omega} : \vec{x} \text{ is linearly dependent in } U\}.$$

Moreover, the Turing degrees of bases of $U$ form exactly the upper cone containing all degrees $\geq_T \deg(D_U)$.

The *canonical basis* for $U$ (using the domain $\omega$) is $\cup_s B_s$, where $B_0 = \emptyset$ and

$$B_{s+1} = \begin{cases} B_s \cup \{s\}, & \text{if this is linearly independent;} \\ B_s, & \text{if not.} \end{cases}$$

This canonical basis is always $\Pi^0_1$ and Turing-equivalent to $D_U$.

# Free abelian groups

The free abelian group on a generating set $L$ is just the set of all finite reduced alphabetized words in the letters from $L$ and their inverses, under concatenation. (A word is *reduced* if it does not contain any substring $xx^{-1}$ or $x^{-1}x$.)

Once again, there is a nice computable presentation $A_\omega$ of this group. In fact, we can just take it to be the subgroup of $V_\omega$ containing those tuples in $\mathbb{Z}^{<\omega}$. (Since this is a computable subset of $V_\omega$, we can index its elements by $\omega$.) The same basis $B_0$ from $V_\omega$ is now computable within $A_\omega$.

Now we must decide: does "basis" refer to a maximal independent set within $A_\omega$, or to an independent set which generates $A_\omega$ (as an abelian group)? Is $2B_0$ a basis for $A_\omega$ or not?

# Results for free abelian groups

## Proposition

Every computable presentation $C$ of the free abelian group $\mathbb{Z}^{<\omega}$ has a $\Pi^0_1$ maximal independent set, which may be taken to be of the same Turing degree as the *dependence relation* on $C$:

$$D_C = \{(x_1, \ldots, x_n) \in C^{<\omega} : \vec{x} \text{ is } \mathbb{Z}\text{-dependent in } C\}.$$

Moreover, the Turing degrees of maximal independent subsets of $C$ form exactly the upper cone containing all degrees $\geq_T \deg(D_C)$.

Every such $C$ also has a $\Pi^0_1$ independent generating set, Turing-equivalent to the *extendibility relation* on $C$:

$$E_C = \{(x_1, \ldots, x_n) \in C^{<\omega} : \vec{x} \text{ extends to an indep. generating set}\}.$$

Moreover, the Turing degrees of independent generating sets of $C$ form exactly the upper cone containing all degrees $\geq_T \deg(E_C)$.

# Distinguishing the two notions

**Theorem**

For every two $\Pi^0_1$ Turing degrees $\boldsymbol{d} \leq_T \boldsymbol{c}$, there exists a computable presentation of $A_\omega$ in which the dependence relation is of degree $\boldsymbol{d}$ and the extendibility relation is of degree $\boldsymbol{c}$.

# More free structures

## Definition

- The *free group* $F_\omega$ on countably many generators $g_i$ is the set of all (finite) reduced words in the alphabet $g_0, g_1, \ldots$ and their inverses, under the operation of concatenation. $F_\omega$ is sometimes denoted by $\langle g_0, g_1, \ldots \rangle$.
- The "free field" $K_\omega$ (of characteristic 0) is the purely transcendental extension of $\mathbb{Q}$ by a countable, algebraically independent set $\{b_0, b_1, \ldots\}$. Elements of $K_\omega$ are just rational functions of these $b_i$ with coefficients in $\mathbb{Q}$. $K_\omega$ is sometimes denoted $\mathbb{Q}(b_0, b_1, \ldots)$.

In both cases, the generating sets are independent: there are no algebraic relations on them except those dictated by the axioms for groups and for fields. Both of these structures can be computably presented with the generating set also computable.

# Bases for these structures

| $K_\omega = \mathbb{Q}(b_0, b_1, \ldots)$ | Free group $F_\omega = \langle g_0, g_1, \ldots \rangle$ |
|---|---|
| $\{b_0, b_1, \ldots\}$ is a **pure transcendence basis**: an independent set generating $K_\omega$. | Group theorists call $\{g_0, g_1, \ldots\}$ a **basis**: an independent set generating $F_\omega$. |

# Bases for these structures

| $K_\omega = \mathbb{Q}(b_0, b_1, \dots)$ | Free group $F_\omega = \langle g_0, g_1, \dots \rangle$ |
|---|---|
| $\{b_0, b_1, \dots\}$ is a **pure transcendence basis**: an independent set generating $K_\omega$. | Group theorists call $\{g_0, g_1, \dots\}$ a **basis**: an independent set generating $F_\omega$. |
| $\{b_0^2, b_1^2, \dots\}$ is a **transcendence basis**: a maximal independent set in $K_\omega$. | $\{g_0^2, g_1^2, \dots\}$ is a... ... |

# Bases for these structures

| $K_\omega = \mathbb{Q}(b_0, b_1, \ldots)$ | Free group $F_\omega = \langle g_0, g_1, \ldots \rangle$ |
|---|---|
| $\{b_0, b_1, \ldots\}$ is a **pure transcendence basis**: an independent set generating $K_\omega$. | Group theorists call $\{g_0, g_1, \ldots\}$ a **basis**: an independent set generating $F_\omega$. |
| $\{b_0^2, b_1^2, \ldots\}$ is a **transcendence basis**: a maximal independent set in $K_\omega$. Field theorists call this a **basis.** | $\{g_0^2, g_1^2, \ldots\}$ is a. . . . . . maximal independent set in $F_\omega$. Group theorists don't call this anything. |

Why the difference? What can computable model theory tell us about the analogies here?

# Transcendence bases for $K_\omega$ are nice

**Facts about transcendence bases $B$ for computable fields $K$**

- $K$ always has a $\Pi^0_1$ transcendence basis.
- $K$ may fail to have a $\Sigma^0_1$ basis (including $K \cong K_\omega$).
- Every transcendence basis for $K$ computes the *dependence set*

$$D_K = \{S \in K^{<\omega} : S \text{ is algebraically dependent over } \mathbb{Q}\}.$$

For $S$ to be dependent over $\mathbb{Q}$ is $\Sigma^0_1$. Conversely, $S = \{x_1, \ldots, x_n\} \in D_K$ iff there exist $b_1, \ldots, b_m \in B$ and $x_{n+1}, \ldots, x_m \in K$ s.t. every $b_i$ ($j \leq m$) is algebraic over $\{x_1, \ldots, x_m\}$.

# Transcendence bases for $K_\omega$ are nice

**Facts about transcendence bases $B$ for computable fields $K$**

- $K$ always has a $\Pi^0_1$ transcendence basis.
- $K$ may fail to have a $\Sigma^0_1$ basis (including $K \cong K_\omega$).
- Every transcendence basis for $K$ computes the *dependence set*

$$D_K = \{S \in K^{<\omega} : S \text{ is algebraically dependent over } \mathbb{Q}\}.$$

For $S$ to be dependent over $\mathbb{Q}$ is $\Sigma^0_1$. Conversely, $S = \{x_1, \ldots, x_n\} \in D_K$ iff there exist $b_1, \ldots, b_m \in B$ and $x_{n+1}, \ldots, x_m \in K$ s.t. every $b_i$ ($j \leq m$) is algebraic over $\{x_1, \ldots, x_m\}$.

**Spectrum of degrees of bases for $K$**

For computable fields $K$ of infinite transcendence degree, $\{\deg(B) : B \text{ is a basis for } K\}$ is just the upper cone above $\deg(D_K)$.

# Bases for $F_\omega$ are somewhat nice

### Facts about bases $B$ for computable free groups $G \cong F_\omega$

- $G$ always has a $\Pi^0_2$ basis (CHKLMMQSW, TAMS 2012).
- $G$ may fail to have a $\Sigma^0_2$ basis (McCoy-Wallbaum, TAMS 2012).
- Every basis $B$ for $G$ computes the set

$$E_G = \{S \in G^{<\omega} : S \text{ extends to a basis for } G\}.$$

The proof that $E_G \leq_T B$ uses the *Nielsen transformations*, which require a basis for $G$ as an oracle. We also use the fact that $F_m \cong F_n \implies m = n$.

### Spectrum of degrees of bases for $G$

For computable groups $G \cong F_\omega$, $\{\deg(B) : B \text{ is a basis for } G\}$ is just the upper cone above $\deg(E_G)$.

# Upper cone results

To show that the spectrum of Turing degrees of bases is the upper cone above $\boldsymbol{d}$, one needs a coding argument for oracles $C$ above $\boldsymbol{d}$. The argument is the same for computable groups $G \cong F_\omega$ (with $\boldsymbol{d} = \deg(E_G)$) as for computable fields $K \cong K_\omega$ (with $\boldsymbol{d} = \deg(D_K)$).

For computable free groups $G$, one builds a canonical transcendence basis $B_0 \equiv_T E_G$, putting $x$ into $B_0$ iff $\{x\} \cup (B_0 \restriction x)$ extends to a basis for $G$. Every oracle $C \geq_T E_G$ computes $B_0 = \{b_0 < b_1 < \cdots\}$, and $C$ is Turing-equivalent to the basis

$$B = \{b_0\} \cup \{b_{i+1} : i \in C\} \cup \{b_0 b_{i+1} : i \notin C\}.$$

# Maximal independent subsets of $G \cong F_\omega$

Let $D_G = \{S \in G^{<\omega} : S \text{ is dependent in } G\}$. Clearly $D_G$ computes a $\Pi^0_1$ maximal independent set.

Natural conjecture: the degrees of maximal independent sets in $G$ comprise the upper cone above $\deg(D_G)$, just as with $E_G$ (for groups) and as with $D_F$ (for maximal independent subsets of the free field $K_\omega$).

# Maximal independent subsets of $G \cong F_\omega$

Let $D_G = \{S \in G^{<\omega} : S \text{ is dependent in } G\}$. Clearly $D_G$ computes a $\Pi^0_1$ maximal independent set.

Natural conjecture: the degrees of maximal independent sets in $G$ comprise the upper cone above $\deg(D_G)$, just as with $E_G$ (for groups) and as with $D_F$ (for maximal independent subsets of the free field $K_\omega$).

**Theorem (McCoy-Miller)**

There exists a computable group $G \cong F_\omega$ with $D_G$ noncomputable, such that $G$ contains a computable maximal independent subset.

So the natural conjecture is false! This gives a quantitative distinction between free groups and free fields.

# A computable group $G$ with $D_G \not\leq_T \emptyset$...

We ensure that no c.e. set $W_e$ can equal $\overline{D_G}$ in our $G$. $G$ will be generated by $\{a\} \cup \{b_e, c_e, d_e : e \in \omega\}$. All these elements will be independent, except for those $d_e$ used to diagonalize against $W_e$; then we have $d_e \in \langle b_e, c_e \rangle$. Thus $G \cong F_\omega$.

Wait for $W_e$ to enumerate the set $\{b_e, c_e, d_e\}$. If it does, we apply:

**Lemma**

Let $n \geq 0$, and fix any finite subset $Y_0$ of the free group $F_3$ on the letters $\{b, c, d\}$, such that $Y_0$ does not contain the identity element. Then there exists a group homomorphism $h : F_3 \to F_2 = \langle b, c \rangle$ with $h(b) = b$, $h(c) = c$, and $Y_0 \cap \ker(h) = \emptyset$. Indeed, we can simply map $d \mapsto c^m b c^{-m}$ for a sufficiently large $m$.

So $\{b_e, c_e, d_e\} \in D_G$ iff $\{b_e, c_e, d_e\} \in W_e$, forcing $W_e \neq \overline{D_G}$.

# ...with a computable maximal independent subset

The group $G$ built above has a basis consisting of $a$, all $b_e$ and $c_e$, and certain $d_e$. The following set is maximal independent in $G$:

$$J = \{waw^{-1} : w \in \langle b_e, c_e, d_e \ : \ e \in \omega\rangle\}.$$

Our diagonalizations leave the subgroup $H = \langle b_e, c_e, d_e \ : \ e \in \omega\rangle$ fixed, so $J$ is computable. Also, every word $u \in G$ differs by a single element $w \in H$ from a word in $\langle J\rangle$. Example:

$$\begin{aligned} u &= b_1 d_3 \cdot a \cdot c_2 \cdot a^{-1} \cdot d_2 \\ &= \underbrace{(b_1 d_3 \cdot a \cdot d_3^{-1} b_1^{-1})}_{v_0 \in J} \cdot \underbrace{(b_1 d_3 c_2 \cdot a^{-1} \cdot c_2^{-1} d_3^{-1} b_1^{-1})}_{v_1 \in J^{-1}} \cdot \underbrace{(b_1 d_3 c_2 d_2)}_{w \in H} \end{aligned}$$

$$\text{So} \quad (v_1^{-1})(v_0^{-1}) \cdot u \cdot (w^{-1} a w) u^{-1} (v_0)(v_1) = a$$

and we have a nontrivial relation on $u$ and elements of $J$.

# Further results and questions on free groups

**Theorem (McCoy-Miller)**

There exists a computable group $G \cong F_\omega$ in which no maximal independent set is c.e. (so $\overline{D_G}$ is noncomputable, hence not c.e.).

The proof adapts the techniques of the previous argument.

The previous theorem showed that $\deg(D_G)$ need not be the least degree in the spectrum of degrees of maximal independent subsets of $G$. Must a least degree exist?

**Conjecture**

There exists a computable group $G \cong F_\omega$ in which no maximal independent set is c.e., yet some two maximal independent sets $I$ and $J$ have infimum $\mathbf{0}$. It would follow that in this $G$, there is no maximal independent set of least degree.

# The remaining quadrant

What about pure transcendence bases for the “free field” $K_\omega$? All questions about this topic are wide open. We have disproven the obvious conjecture:

**Theorem (Kramer & others)**

There exists a finite independent subset $S \subseteq K_\omega$ which does not extend to a pure transcendence basis, yet every element of $K_\omega$ which is algebraic over $S$ is generated by $S$.

Fix a computable $K \cong K_\omega$ with a computable PTB. Let $E_K$ be the set of finite subsets of $K$ which extend to PTBs for $K$. As of now, $E_K$ is known to be somewhere between $\Pi^0_1$ and $\Sigma^1_1$.