**Ehrenfeucht’s Conjecture**

- It was conjectured by Ehrenfeucht in the beginning of 1970s in a language theoretic setting.


- Proved by Albert and Lawrence and independently by Guba (1985).

- Techniques originated by Markov (1950's).

- Known also as Compactness theorem (for equations) and Noetherian property (of equations).

**Equality sets**

A **morphism** $\alpha : A^* \to B^*$ satisfies

$$\alpha(uv) = \alpha(u)\alpha(v).$$

Therefore morphisms are determined by their images of the letters $a \in A$.

We need only specify $\alpha(a)$ for each letter $a$:

$$\alpha(w) = \alpha(a_{i_1}a_{i_2} \ldots a_{i_n}) =$$

$$\alpha(a_{i_1})\alpha(a_{i_2}) \ldots \alpha(a_{i_n})$$

whenever $w = a_{i_1}a_{i_2} \ldots a_{i_n}$.

**Example.** $A = \{a, b\}$ and $B = \{a, b, c\}$.
Let $\alpha(a) = ab$ and $\alpha(b) = aca$.
Then $\alpha(aba) = abacaab$. 
Let $\alpha, \beta: A^* \to B^*$ be morphisms. Their equality set is

$$E(\alpha, \beta) = \{w \in A^+ | \alpha(w) = \beta(w)\}.$$ 

That is, $E(\alpha, \beta)$ is the set of all (nonempty) words upon which $\alpha$ and $\beta$ agree.

**Lemma 1.** $E(\alpha, \beta)$ is a free semigroup, for which

$$v, uv \in E(\alpha, \beta) \implies u \in E(\alpha, \beta)$$

$$u, uv \in E(\alpha, \beta) \implies v \in E(\alpha, \beta).$$

**Example.**

- Let $A = \{a, b\}$. Consider $\alpha, \beta: A^* \to A^*$, where

  $$\alpha(a) = aba \quad \alpha(b) = ba$$
  $$\beta(a) = ab \quad \beta(b) = aba.$$

  For instance, $ab \in E$: $\alpha(ab) = aba \cdot ba = ab \cdot aba = \beta(ab)$. In this example

  $$E = (ab)^+ = \{(ab)^n | n \geq 0\}.$$ 

- Let $A = \{a, b, c\}$, and $\alpha, \beta: A^* \to A^*$:

  $$\alpha(a) = ab \quad \alpha(b) = bb \quad \alpha(c) = c$$
  $$\beta(a) = a \quad \beta(b) = bb \quad \beta(c) = bc$$

  In this case

  $$E(\alpha, \beta) = b^+ \cup ab^*c.$$
Remark. The problem whether $E(\alpha, \beta) = \emptyset$ is algorithmically undecidable.

This is the Post correspondence problem. There are thus arbitrarily complex equality sets.

Example. Consider

$$\alpha(a) = a, \quad \alpha(b) = b, \quad \alpha(c) = abb,$$
$$\beta(a) = b, \quad \beta(b) = abb, \quad \beta(c) = a.$$ 

Then $E(\alpha, \beta) \neq \emptyset$.
The minimum word $w$ has length

$$|w| = 75$$

Test sets

This is the original conjecture by Ehrenfeucht:

**Theorem 1. [Ehrenfeucht’s conjecture]**

Let $L \subseteq A^*$. There exists a finite subset $T \subseteq L$ such that for all morphisms $\alpha, \beta : A^* \to B^*$

$$\alpha|T = \beta|T \iff \alpha|L = \beta|L.$$ 

The subset $T$ is a test set of $L$.

To check if two morphisms agree on $L$, it suffices to check if they agree on the finite subset $T$. 
Theorem 1 may be restated:

**Theorem 2.** Let $L \subseteq A^*$. There exists a finite subset $T \subseteq L$ such that for all morphisms $\alpha, \beta : A^* \to B^*$

$$T \subseteq E(\alpha, \beta) \iff L \subseteq E(\alpha, \beta).$$

**Example.** Let $L = \{a^n b^n \mid n \geq 1\}$.

Then $T = \{ab, a^2b^2\}$ is a test set of $L$.

It is of the smallest size.

---

**Equations**

Let

$$X = \{x_1, x_2, \ldots, x_n\}$$

be a special alphabet of **variables**.

An equation over $X$ is a pair $(u, v)$ (for $u, v \in X^+$).

Write

$$u = v$$

for $(u, v)$.

A sequence \((w_1, w_2, \ldots, w_n)\) \((w_i \in A^*)\) is a solution of $u = v$, if the substitution $x_i \mapsto w_i$ in $u$ and $v$ results in the same word of $A^*$. 
In other words,

A solution of \( u = v \) is a morphism \( \alpha: X^* \to A^* \) such that \( \alpha(u) = \alpha(v) \).

(\( \text{Set } \alpha(x_i) = w_i. \))

All equations have the trivial solution:

\[ \alpha(x) = \lambda \quad \text{for all } x \in X. \]

**Example.** The equation \( x = x^2 \) has no other solution than the trivial one, since a solution \( x \mapsto w \) has to satisfy \( 2 \cdot |w| = |w| \).

**Example.** Let \( X = \{x, y, z\} \), and consider

\[ xyx = zyxz \]

Let \( x \mapsto u, y \mapsto v, z \mapsto w \) be a solution.

By comparing the lengths: \( |uvw| = |wvw| \),

\[ 2|u| + |v| = |u| + |v| + 2|w| \implies |u| = 2|w| \]

and \( u = wv_0 \) for \( |w_0| = |w| \). Then

\( w_0vww_0 = wvwvv_0w \), i.e., \( vvv_0v_0w = vwwvw_0 \).

By the suffixes, \( w_0 = w \). Thus \( vvv = vv \).

Now \( v \) and \( w \) are powers of the same word, say \( v = u_0^r \) and \( w = u_0^s \).

Hence \( u = wv_0 = vv = u_0^{2s} \).

Also, if \( u_0 \) is any word, then \( u = u_0^{2s}, v = u_0^r, w = u_0^s \) is a solution for any \( r, s \geq 0 \).

We have found all the solutions of the equation.
A set of equations (in variables from X)

\[ E = \{(u_i, v_i) \mid i = 1, 2, \ldots\} \]

is a system of equation.
A solution of \( E \) is a common solution to all \( u_i = v_i \).

**Example.** Let \( X = \{x_1, x_2, y_1, y_2\} \). Consider

\[ x^i y^i_1 = x^i y^i_2 \quad (i \geq 1). \]

This system of equations has the solutions

\[ \alpha(x_1) = w_1 = \alpha(x_2), \quad \alpha(y_1) = w_2 = \alpha(y_2). \]

Also, \( \beta(x_1) = aa, \quad \beta(x_2) = a, \quad \beta(y_1) = a, \quad \beta(y_2) = aa \) is a solution.

Two systems \( E_1 \) and \( E_2 \) of equations are equivalent, if they have the same solutions.

**Example.** The system \( E \)

\[ xy^i = z^ix \quad (i = 1, 2, \ldots) \]

is equivalent to the single equation

\[ xy = zx. \]

Indeed:

Let \( x \mapsto u, \ y \mapsto v, \ z \mapsto w \)
be a solution of \( xy = zx \): \( uv = wu \). Then

\[ uv^i = uv \cdot v^{i-1} = wu \cdot v^{i-1} = \cdots = w^i u. \]

Note also that \( uv = wu \) implies

\[ v = rs, \ w = sr, \ u = (sr)^k s \]

for some words \( r, s \) and integer \( k \geq 0 \).
A system $E$ is **independent** if it is not equivalent to any of its proper subsystems.

**Example.** Let

$$E: \quad xyz = zyx, \quad xy^2z = zy^2x$$

Then $E$ is independent:

- $x \mapsto a$, $y \mapsto b$ and $z \mapsto aba$ is a solution of the first equation, but not of the second.

- $x \mapsto a$, $y \mapsto b$ and $z \mapsto abba$ is a solution of the second, but not of the first one.

**Example.** Is the system

$$xyz = zyx, \quad xy^2z = zy^2x, \quad xy^3z = zy^3x$$

independent?

**Theorem 3.** Ehrenfeucht’s conjecture is equivalent to

\[(*) \text{ Every system of equations } E \text{ is equivalent to a finite subsystem } E_T \subseteq E.\]

**Proof.** [Idea] For any alphabet $B$, let $\overline{B} = \{\overline{a} \mid a \in B\}$ be a new alphabet, and let $\overline{u} = \overline{a_1a_2 \ldots a_k} \in \overline{B}^+$ for $u = a_1a_2 \ldots a_k \in B^+$.

1. For a system of equations $u_i = v_i$ consider the language

$$L = \{u\overline{v} \mid u = v \in E\} \subseteq (X \cup \overline{X})^*.$$

2. For a language $L$, consider the set of equations

$$E = \{(u, \overline{u}) \mid u \in L\}.$$

\qed
Hilbert’s basis theorem

In the proof of Ehrenfeucht’s conjecture we need the original version of Hilbert’s basis theorem.

Let \( \mathbb{Z}[x_1, x_2, \ldots, x_n] \) be the ring of polynomials with integer coefficients in (commuting) variables \( x_1, x_2, \ldots, x_n \).

**Theorem 4.** Each system of equations

\[ P_i = 0 \quad (P_i \in \mathbb{Z}[x_1, x_2, \ldots, x_n]) \]

has a finite equivalent subsystem.

The result

**Theorem 5.** Every independent system of equations in a free semigroup \( A^+ \) over a finite set \( X \) of variables is finite.

**Theorem 6.** Every system of equations in \( A^+ \) over a finite set \( X \) of variables has a finite equivalent subsystem.

**Idea of the proof:**

Transform each word equation into a polynomial equation in \( \mathbb{Z}[Y] \) (using matrices of integer polynomials).

\[ u = v \quad \iff \quad P(x_1, \ldots, x_k) = 0 \]

\( X = \{x_1, x_2, \ldots, x_k\} \) is a set of word variables.
Reduce images to binary case

Each $A^+$ embeds into $B^+$ for $B = \{a, b\}$:

$$a_i \mapsto a^i b$$

Sufficient to solve equations over $B^+$:

$$\alpha : X^+ \to B^+$$

Indeed, let $A = \{a_1, a_2, \ldots, a_m\}$, and

$$\beta : A^* \to B^*, \beta(a_i) = a^i b.$$

Let $\alpha : X^* \to A^*$.

Then $\alpha(u) = \alpha(v)$ iff $\beta \alpha(u) = \beta \alpha(v)$.

Here $\beta \alpha : X^* \to B^*$.

Reduce images to matrices

Let $\mathbb{F} \subseteq \mathbb{Z}^{2 \times 2}$ consist of the matrices

$$M = \begin{pmatrix} 2^m & n \\ 0 & 1 \end{pmatrix} \quad 0 \leq n < 2^m, \ 1 \leq m$$

**Theorem 7.** $\mathbb{F}$ is a free semigroup.

*It is isomorphic to $\{a, b\}^+$:

$$\mu : \{a, b\}^+ \to \mathbb{F} \subseteq \mathbb{Z}^{2 \times 2}$$

where

$$\mu(a) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \mu(b) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$
Reduce domain to matrices

For \( x_i \in X \) introduce two commuting integer variables \( y_i, z_i \):

\[
Y = \{y_i, z_i \mid i = 1, 2, \ldots, k\}
\]

For each \( i \):

\[
M_i = \begin{pmatrix} y_i & z_i \\ 0 & 1 \end{pmatrix}
\]

Let

\[
\mathbb{M}(X) \subseteq \mathbb{Z}[X]^{2 \times 2}
\]

be the semigroup generated by \( M_1, M_2, \ldots, M_k \).

**Theorem 8.** The semigroup \( \mathbb{M}(X) \) is free. It is isomorphic to \( X^+ \):

\[
\varphi : X^+ \to \mathbb{M}(X)
\]

where

\[
\varphi(x_i) = M_i
\]

The diagram

For \( \alpha : X^+ \to B^+ \) let

\[
\bar{\alpha} = \mu \alpha \varphi^{-1} : \mathbb{M}(X) \to \mathbb{Z}^{2 \times 2}
\]

\[
\begin{array}{ccc}
X^+ & \xrightarrow{\alpha} & B^+ \\
\varphi \downarrow & & \mu \downarrow \\
\mathbb{M}(X) & \xrightarrow{\bar{\alpha}} & \mathbb{Z}^{2 \times 2} \\
\downarrow & & \downarrow \\
\mathbb{Z}[Y]^{2 \times 2} & & \\
\end{array}
\]
For each word $w \in X^+$, let the polynomials $P_1(w), P_2(w) \in \mathbb{Z}[Y]$ be defined by

$$\varphi(w) = \begin{pmatrix} P_1(w) & P_2(w) \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}[Y]^{2 \times 2}.$$ 

Let $\hat{\alpha} : \mathbb{Z}[Y] \to \mathbb{Z}$ be the ring morphism:

$$\hat{\alpha}(M_i) = \begin{pmatrix} \hat{\alpha}(y_i) & \hat{\alpha}(z_i) \\ 0 & 1 \end{pmatrix}$$

So

$$\hat{\alpha}\varphi(w) = \begin{pmatrix} \hat{\alpha}(P_1(w)) & \hat{\alpha}(P_2(w)) \\ 0 & 1 \end{pmatrix}$$

Hence

$$\alpha : X^+ \to B^+ \text{ solution of } u = v$$

iff

$$\hat{\alpha} \text{ solution of } \varphi(u) = \varphi(v)$$

iff

$$\hat{\alpha} : \mathbb{Z}[Y] \to \mathbb{Z} \text{ solution of }$$

$$\left\{ \begin{array}{l} P_1(u) = P_1(v) \\ P_2(u) = P_2(v) \end{array} \right.$$}

iff

$$\hat{\alpha} : \mathbb{Z}[Y] \to \mathbb{Z} \text{ solution of } e(u, v) = 0$$

where

$$e(u, v) = (P_1(u) - P_1(v))^2 + (P_2(u) - P_2(v))^2.$$
Let
\[ E = \{(u_i, v_i) \mid i \geq 1\} \]
be a system of word equations.

Let
\[ J = \{e(u_i, v_i) \mid i \geq 1\} \]
be the corresponding polynomial equations.

By HBT, \( J \) has an equivalent finite subsystem
\[ J_0 = \{e(u_i, v_i) \mid i = 1, 2, \ldots, t\} \]

If \( \alpha \) is a solution of
\[ E_0 = \{(u_i, v_i) \mid i = 1, 2, \ldots, t\} \]
then \( \hat{\alpha} \) is a solution of \( J_0 \), and thus of \( J \), and so \( \alpha \) is a solution of \( E \).

Hence \( E_0 \) is equivalent to \( E \).

This proved EC.

Applications

The original conjecture follows:

**Theorem 9.** Every language \( L \subseteq A^+ \) has a finite test set.

The next corollary needs more proving.

**Theorem 10.** For finite sets \( X, Y \subseteq A^+ \), it is decidable whether the semigroups \( X^+ \) and \( Y^+ \) are isomorphic.
Application: Endomorphism monoids

An endomorphism is a morphism \( \alpha: A^+ \to A^+ \).

**Theorem 11.** Let \( H \) be a monoid of generated by finitely many endomorphisms of \( A^+ \). Let also \( w \in A^+ \). It is decidable for endomorphisms \( \alpha, \beta \) of \( A^* \), whether

\[
\alpha \gamma(w) = \beta \gamma(w)
\]

for all \( \gamma \in H \).

Application: DTOL problem

In the DTOL problem given are a word \( w \in A^+ \), two monoids \( H_1 \) and \( H_2 \) of endomorphisms of \( A^* \) with equally many generators

\[
\{ \alpha_1, \alpha_2, \ldots, \alpha_n \}
\]

\[
\{ \beta_1, \beta_2, \ldots, \beta_n \}
\]

We ask whether for all sequences \( i_1, i_2, \ldots, i_k \) of indices,

\[
\alpha_{i_k} \ldots \alpha_{i_1}(w) = \beta_{i_k} \ldots \beta_{i_1}(w).
\]

**Theorem 12.** The DTOL problem is decidable.

The (only known) proof is based on Makanin’s algorithm and the compactness property.

Its special case, the DOL problem, where \( H_1 \) and \( H_2 \) are both generated by a single morphism, has several different proofs.