Termination of original F5

Vasily Galkin
galkin-vv@yandex.ru

Moscow State University
Faculty of Mechanics and Mathematics
Department of Higher Algebra

Main goal

Prove that F5 algorithm terminates on any input data represented by a set of homogeneous polynomials.

1. Definitions
   - Polynomial signature
   - Algorithm F5: original version
2. Termination proof
   - F5 terminates: scheme of proof
   - S-pair chains
   - Representations of p with $\mathcal{S}(p) \prec \mathcal{S}(h)$

Polynomial signature

- Fix ideal generated by "input" polynomials $I = (f_1, \ldots, f_n)$
- Fix order $\prec$ on pairs (m, f_i); m is monomial without coefficient

Definitions

Signature: $\max_\prec (m_k, f_{i_k})$ for some input-representation

$$g = \sum_k c_k m_k f_{i_k},\ c_k \neq 0, \text{ all pairs } (m_k, f_{i_k}) \text{ are distinct}$$

Minimal signature: $\mathcal{S}(g) \stackrel{\text{def}}{=} min_\prec$ (all signatures of g)

We say *mh sig-safe reduce g* if $\mathrm{LM}(mh) = \mathrm{LM}(g)$, $\mathcal{S}(mh) \prec \mathcal{S}(g)$

- F5 tracks $\mathcal{S}$ and performs only signature-safe reductions
- F5 use Position-over-Term order $\prec$ (compare i-s than m-s)
  - Order is compatible to multiplication by monomial
  - Allows to define *sig-lead ratio* with linear order:

$$\frac{\mathcal{S}(g)}{\mathrm{LM}(g)} \prec_{SL} \frac{\mathcal{S}(h)}{\mathrm{LM}(h)} \stackrel{\text{def}}{\Leftrightarrow} \mathcal{S}(g)\,\mathrm{LM}(h) \prec \mathcal{S}(h)\,\mathrm{LM}(g)$$

Algorithm F5: original version

Scheme: computing basis of $(G \cup \{f_i\})$ from basis G

1. $P = \{\text{S-pair}(p, f_i) | p \in G$, and S-pair parts pass 'F5' criterion$\}$
2. **while** $P \neq \varnothing$ **do:**
    - 2.1 $F =$ S-polys(take P all max-degree S-pairs passing 'Rewritten')
    - 2.2 **while** $\exists h \in F$, $\mathcal{S}(h)$ is minimal for non-zero F polynomials **do:**
        - 2.2.1 **if** $\exists p \in G$ – sig-safe h reductor, satisfying 'F5' and 'Rewritten'**:** $F = (F \setminus \{h\}) \cup$Reduce(h,p)
        - 2.2.2 **else:** $F = F \setminus \{h\}$; $R = R \cup \{h\}$
    - 2.3 **for** $r \in R$**:**$P = P \cup \{\text{S-pair}(p, r) | p \in G, \text{'F5' passed}\}$; $G = G \cup \{r\}$

Termination of original F5

- is topical: no algorithm was proved to be always faster than F5
- is not like Buchberger: G may be extended by polynomial h whose reductor $p \in G$ is not sig-safe or is not satisfying criteria
- proofed in original work only if $f_1, \ldots, f_n$ is regular sequence
- proof by reformulation as generic algorithm (TRB-F5; F5GEN)
    - equivalence proof has gaps

F5 terminates: scheme of proof

1* If the algorithm doesn't stop it fills G with polynomials containing infinite sequence with $\prec_{SL}$-increasing sig-lead ratio

2 This sequence contains p_1, p_2 with $\mathrm{LM}(p_2)|\mathrm{LM}(p_1)$

3 Polynomial p_2 is sig-safe reductor for p_1

4* Any polynomial p with signature smaller than signature of h on step 2.2 has representation of the form $p = \sum_k c_k m_k g_k,\ c_k \neq 0, g_k \in G$ where $\mathcal{S}(m_k g_k) \preccurlyeq \mathcal{S}(p), \mathrm{LM}\,(m_k g_k) \leqslant \mathrm{LM}\,(p)$ and all $m_k g_k$ satisfy F5 and Rewritten criteria

5 Applying this to p_2 on step with $h = p_1$ and selecting element with $\mathrm{LM}\,(m_k g_k) = \mathrm{LM}\,(p_2)$ as mp_3 gives polynomial p_3 in G.

6 p_3 is sig-safe reductor of p_1 and satisfies criteria

7 This leads to contradiction because p_1 was added to G without reduction by p_3

**studied below in more detail*

S-pair chains

Definitions

- Polynomial h_2 computed as reduced S-pair(h_1, p) satisfying $\mathcal{S}\left(\mathrm{LM}\left(p\right) h_1\right) \succ \mathcal{S}\left(\mathrm{LM}\left(h_1\right) p\right)$ is called *S-descendant* of h_1.
- *S-descendant property*: $h_2 \succ_{SL} h_1$
- Sequence $\{h_i\}$ is *S-pair chain*, if $\forall i\, h_{i+1}$ is S-descendant of h_i.

Fact

If F5 doesn't stop it gives infinite S-pair chain

Proof.

- All $h \in R$ corresponds to S-pair chain $\{f, \ldots, h\}$
- $\forall h$ has only finite number of direct S-pair descendants
- A chain is constructed from elements having infinite number of recursive S-pair descendants

□

Representations of p with $\mathcal{S}(p) \prec \mathcal{S}(h)$

$\forall p$ has representation $p = \sum_k c_k m_k g_k$, $c_k \neq 0, g_k \in G$, satisfying:

- $\mathrm{LM}(p) \geqslant \mathrm{LM}(m_k g_k)$ – all algorithms, including Buchberger
- $\mathcal{S}(p) \geqslant \mathcal{S}(m_k g_k)$ (sig-safe) – all signature-based algorithms
- For F5 we also need to analyze 'F5' and 'Rewritten' criteria
  - start with a sig-safe representation
  - iteratively replace terms that doesn't pass criteria or LM relation with sig-safe expressions
  - proof that this process terminates

Proof.

- Introduce well order $\lessdot_1$ on representation elements (like $\prec$)
- Lexicographically extend it to representations well order $\lessdot$
- Show that replacements $\lessdot$-decrease representation

□