Proof of Dickson's lemma in ACL2 via an explicit ordinal mapping

by Mátyás Sustik

I present the use of the ACL2 theorem prover to formalize and mechanically check a new proof of Dickson's lemma about monomial sequences. Dickson's lemma can be used to establish the termination of the Buchberger algorithm to find the Gröbner basis of a polynomial ideal. This effort is related to a larger project which aims to develop a mechanically verified computer algebra system.

Contents

Background

- A (polynomial) ideal I of an R ring is defined as a subset closed under subtraction and under multiplication with arbitrary elements of R. $i_1, i_2 \in I$, $r \in R \Longrightarrow i_1 - i_2 \in I, ir, ri \in I$.
- Classic example: modulo arithmetic in $\mathbb{Z}$. The ideal generated by 5 is the set: $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$.
- Another example: the ideal generated by x^2 and $3x$ in $\mathbb{Z}[x]$, the ring of polynomials with integer coefficients consists of the polynomials which have a constant coefficient equal to 0 and the coefficient of x is divisible by 3.

$$x^3 + 2x^2 + 6x = (x + 2) \cdot x^2 + 2 \cdot 3x.$$

- The Gröbner basis is a uniquely determined special basis for a polynomial ideal; its determination helps to decide equality of ideals presented with arbitrary generators.
- Buchberger's algorithm takes an ideal given by a generator set and calculates the Gröbner basis.
- The termination of the algorithm is established by Dickson's lemma.
- Keith O. Geddes and S. R. Czapor and G. Labahn: Algorithms for Computer Algebra

Dickson's lemma

- We consider terms over a finite set of symbols e.g.: $x_0^2 x_1 x_2^3$.
- A monomial $x_0^{u_1} x_1^{u_2} \ldots x_{k-1}^{u_{k-1}}$ divides $x_0^{v_0} x_1^{v_1} \ldots x_{k-1}^{v_{k-1}}$ iff $u_i \leq v_i$ for all possible values of i.
- Claim: Given an infinite sequence of monomials: $m_1, m_2, m_3, \ldots$ exist i, j indices such that $i < j$ and m_i divides m_j.
- Classical proofs may use Ramsey's theorem about infinite graphs colored with finitely many colors, or other non-constructive arguments to select certain subsequences.

Dickson's lemma

(auxiliary material)

- Classical proof sketch 1: There is a subsequence $m_{i_1}, m_{i_2}, m_{i_3}, \ldots$ such that the exponent of the first variable in m_{i_j} is (weakly) increasing. Omit the first variable from the terms and restrict to the above subsequence to set the stage for an induction on the number of variables.
- Classical proof sketch 2: Suppose m_i does not divide m_j for any $i < j$. Denote the index of a 'witness' variable by $c(i, j)$: the exponent of the variable is less in m_j than in m_i. Consider the infinite complete graph on the positive integers naturally colored by $c(i, j)$. Ramsey's theorem asserts that there is an infinite uniformly colored complete subgraph, which would imply the existence of an infinite descending sequence of natural numbers, a contradiction.

Ordinals

- Panagiotis Manolios and Daron Vroon: Algorithms for Ordinal Arithmetic, 19th International Conference on Automated Deduction (CADE) 2003
- Additional ordinal lemmas. (About addition, exponentiation, and the notion of less than equal relation among ordinals.)

Ordinals

(auxiliary material)

- Ordinal addition is non-commutative, associative.
- $1 + \omega = \omega < \omega + 1$.
- Exponentiation is monoton.
- If $a_1 \leq a_2$ and $b_1 \leq b_2$ then $a_1 + b_1 \leq a_2 + b_2$.
- Suppose $a_1 < a_2$ and $b_1 \leq b_2$. Does this imply that $a_1 + b_1 < a_2 + b_2$?
- Suppose $a_1 \leq a_2$ and $b_1 < b_2$. Does this imply that $a_1 + b_1 < a_2 + b_2$?

Definition of the mapping

- Build an ordinal mapping which assigns an ordinal to the initial segments of the monomial sequence such that: if no monomial divides another appearing later in the sequence, then the ordinals form a decreasing sequence.

- I represent the monomials as k-tuples and denote by $\mathcal{A}_k$ the collection of finite sets of k-tuples:
$$\mathcal{A}_k = \{A \subset \mathbb{N}^k : |A| < \omega\}.$$

- We define the $M_k : \mathcal{A}_k \to Ord$ function inductively. If $A \in \mathcal{A}_1$ then set
$$M_1(A) = \min A,$$
with the agreement that $M_1(\{\}) = \omega$.

- Now suppose that $k > 1$ and that we have already defined M_{k-1}. For an arbitrary $A \in \mathcal{A}_k$ and $i \in \mathbb{N}$ define the $P_i^{(A)} \in \mathcal{A}_{k-1}$ sets and the $\alpha_i^{(A)}$ ordinals as follows:
$$P_i^{(A)} = \{(u_1, u_2, \ldots, u_{k-1}) : (u_0, u_1, \ldots, u_{k-1}) \in A, u_0 \leq i\},$$
$$\alpha_i^{(A)} = M_{k-1}(P_i^{(A)}).$$

Definition of the mapping

(auxiliary material)

- $M_1(\{3, 5, 2, 7\}) = 2$. Note that $\mathbb{N}^1 = \mathbb{N}$.

- $A = \{(3, 2), (2, 3), (1, 6), (2, 4), (3, 6)\}$.

$$\begin{array}{ll}
P_0^{(A)} = \{\} & \alpha_0^{(A)} = \omega, \\
P_1^{(A)} = \{6\} & \alpha_1^{(A)} = 6, \\
P_2^{(A)} = \{3, 4, 6\} & \alpha_2^{(A)} = 3, \\
P_3^{(A)} = \{2, 3, 4, 6\} & \alpha_3^{(A)} = 2, \\
P_4^{(A)} = \{2, 3, 4, 6\} & \alpha_4^{(A)} = 2.
\end{array}$$

Definition of the mapping

continued

- The P_i, α_i sequences stabilize for every $A \in \mathcal{A}_k$.
- Denote an index by $m = m^{(A)}$ for which $\alpha_i = \alpha_s$ for every $i \geq m$ and define:

$$M_k(A) = \left(\sum_{i=0}^{m-1} \omega^{\alpha_i} \right) + \omega^{\alpha_m + 1}.$$

- Define the partial sums that make up M_k:

$$M_k(A, j) = \begin{cases} \min A & \text{if } k = 1 \\ \left(\sum_{i=j}^{m-1} \omega^{\alpha_i} \right) + \omega^{\alpha_m + 1} & \text{if } k > 1 \end{cases}$$

Definition of the mapping

(auxiliary material)

- $A = \{(3,2), (2,3), (1,6), (2,4), (3,6)\}$, $m = 3$.
- $\alpha_0^{(A)} = \omega$, $\alpha_1^{(A)} = 6$, $\alpha_2^{(A)} = 3$, $\alpha_3^{(A)} = 2$.
- By the definition:

$$M_2(A) = \omega^\omega + \omega^6 + \omega^3 + \omega^3.$$

- The following form reveals the intuition behind the definition:

$$M_2(A) = \omega^\omega + \omega^6 + \omega^3 + \omega^2 + \omega^2 + \dots.$$

Proof

1. If $A \subseteq B \in \mathcal{A}_k$ then $M_k(A) \geq M_k(B)$.
2. For any $A \in A_k$, $k > 1$ the α_i sequence is monotone decreasing.
3. For any $A, B \in \mathcal{A}_k$, $k > 1$, $M_k(A) = M_k(B)$ holds if and only if $\alpha_i^{(A)} = \alpha_i^{(B)}$ is true for every $i \in \mathbb{N}$.
   - Seven further lemmas lead to the proof of the above statement.
   - An induction scheme is specified.
   - Ordinal arithmetic lemmas are instantiated.

Proof

(continued)

4 If $A \subseteq B \in \mathcal{A}_k$, $v \in B \setminus A$ and $M_k(A) = M_k(B)$ then there is a $w \in A$ such that $w \leq_k v$.

- Witness functions are defined to allow formalization of some properties.
- If $x \in P_i^{(A)}$ then there exists a $y \in A$ such that:

$$y = (u_0, u_1, \ldots, u_{k-1}),\;\; u_0 \leq i,\;\; x = (u_1, \ldots, u_{k-1}).$$

5 If $s_1, s_2, \ldots, s_n$ is a finite sequence of k-tuples of natural numbers such that for any $1 \leq i < j \leq n$ we have $s_i \not\leq_k s_j$ then the $M_k(A_1), M_k(A_2), \ldots, M_k(A_n)$ sequence of ordinals is strictly decreasing where A_j denotes an initial segment of s_i: $A_j = \{s_i : 1 \leq i \leq j\}$.

Proof— ACL2 events

(auxiliary material)

```
(defun tuple-set-filter (S i)
  (cond ((endp S) NIL)
        ((and (consp (first S)) (<= (first (first S)) i))
         (cons (first S) (tuple-set-filter (rest S) i)))
        (T (tuple-set-filter (rest S) i))))

(defun tuple-set-projection (S)
  (cond ((endp S) NIL)
        ((consp (first S))
         (cons (rest (first S))
               (tuple-set-projection (rest S))))
        (T (tuple-set-projection (rest S)))))

(defun tuple-set->ordinal-partial-sum (k S i)
  (declare (xargs :measure
   (cons (1+ (nfix k))
         (nfix (- (tuple-set-max-first S) i)))))
  (cond ((or (not (natp k)) (not (natp i))) 0)
        ((zp k) 0)
        ((equal k 1)
         (tuple-set-min-first S))
        ((<= (tuple-set-max-first S) i)
         (o^ (omega)
             (o+ (tuple-set->ordinal-partial-sum
                  (1- k)
                  (tuple-set-projection S)
                  0)
                 1)))
        (T (o+
            (o^ (omega)
                (tuple-set->ordinal-partial-sum
                 (1- k)
                 (tuple-set-filter-projection S i)
                 0))
            (tuple-set->ordinal-partial-sum k S
                                           (1+ i))))))
```

Proof—ACL2 events

(auxiliary material)

```
(defthm map-lemma-3.7
  (implies (and (tuple-setp k A)
                (tuple-setp k B)
                (natp k)
                (< 1 k)
                (natp i)
                (natp j)
                (<= i j)
                (equal
                 (tuple-set->ordinal-partial-sum k A i)
                 (tuple-set->ordinal-partial-sum k B i)))
           (equal (equal (tuple-set->ordinal-partial-sum
                          (1- k)
                          (tuple-set-projection
                           (tuple-set-filter A j))
                          0)
                         (tuple-set->ordinal-partial-sum
                          (1- k)
                          (tuple-set-projection
                           (tuple-set-filter B j))
                          0))
                  T))

(defthm dixon-map-thm
  (implies (and (tuple-setp k S)
                (consp S)
                (natp k)
                (<= 1 k)
                (not (exists-partial-tuple-<=-set
                      k (rest S) (first S))))
           (o< (tuple-set->ordinal k S)
               (tuple-set->ordinal k (rest S)))))
```

Summary

- The need for a machine verified proof of Dickson's lemma lead to a new proof different from the classical ones.
- The effort motivated the development of an ordinal book for ACL2 which may well benefit other proof attempts as well.
- The proof enabled the verification of the termination of the Büchberger algorithm implemented in ACL2.
- Used 23 function definitions two of them ordinal related. Proved 80 theorems of which 26 was ordinal related (not counting the theorems imported from the ordinal book referenced).

Acknowledgments

The author thanks Sandip Ray for sharing his valuable comments and insights which helped to succeed and simplify this proof attempt. Robert Krug and Matt Kaufmann helped with ACL2 problems and questions. The author was glad to cooperate with I. Medina-Bulo and Panagiotis Manolios while working on this project, and to receive the support and encouragement of J Strother Moore.