Low Degree Solutions to Linear Equations with $K[x]$ Coefficients †

M. KALKBRENER‡ M. SWEEDLER‡ L. TAYLOR §

For given $f_1, \ldots, f_m \in K[x]$ which are relatively prime we present degree bounds on the a_i needed to express 1 and other "low degree" polynomials as $\sum a_i f_i$. This paper gives an improvement on Kakié's bound (Kakié, 1976).

1. Introduction

If $f_1, \ldots, f_m \in K[x]$, K a field, are relatively prime then 1 can be expressed as $1 = \sum_{i=1}^{m} a_i f_i$. In Kakié (1976) the bound

$$deg(a_i) < \max_{1 \le j \le m} (deg(f_j)) + \min_{1 \le j \le m} (deg(f_j)) - deg(f_i)$$

is given. This bound can also be found in Shiffman (1989). In this paper we obtain the new bound, G_i,

$$G_1 \le \max_{1 \le j \le m} (deg(f_j)) - T + 1 \quad \text{and} \quad G_i \le \min_{1 \le j \le m} (deg(f_j)) - T + 1 \quad \text{for } i \in \{2, \ldots, m\}$$

on the degree of the a_i, where f_1 is a polynomial of minimal degree among the f_i and no subset of the f_i of cardinality T is relatively prime. We give a class of polynomials for every m in which this bound is attained and prove sharper bounds in a special case.

The question of how to express "1" fits within a natural vector space consideration. For a natural number D we define $K^{(D)} := \{f \in K[x] \mid deg(f) < D\}$. Integers $D_1, \ldots, D_m$ and D give a *degree isomorphism* for $f_1, \ldots, f_m$ if

$$\lambda : K^{(D_1)} \oplus \cdots \oplus K^{(D_m)} \longrightarrow K^{(D)}, \tag{1.1}$$

defined by $\lambda(a_1, \ldots, a_m) = \sum_{i=1}^{m} a_i \cdot f_i$, is a vector space isomorphism. The general degree isomorphism problem is to understand the interrelationship between $D_1, \ldots, D_m$ and D. One possible question is: what is the lowest possible D for given $f_1, \ldots, f_m$? Note that once a degree isomorphism is achieved by a specific D, then for any larger value E there is also a degree isomorphism. Simply choose i where $D_i + deg(f_i)$ is maximal and replace D_i by $D_i + E - D$. The main thrust of this paper is to develop upper and lower bounds for this lowest possible D.

† This work has been supported by the U.S. Army Research Office through the Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), Mathematical Sciences Institute of Cornell University. Contract DAAL03-91-C-0027.

‡ Mathematical Sciences Institute, Cornell University, Ithaca NY 14853.

§ Department of Defense and Mathematical Sciences Institute, Cornell University.

We have two approaches. One uses easy results about modules. The other is even easier. Using results about modules we obtain an upper bound for this lowest possible D. It is this result which gives the improvement on Kakié's bound for expressing "1". It is worth noting that even for two polynomials one may have $1 = \sum a_i f_i$ with strictly better bounds on the a_i than for the vector space isomorphism. For example, with $f_1 := 1 - x^2$ and $f_2 := x^2$ the polynomial 1 can be represented in the form $a_1 f_1 + a_2 f_2$ with constant a_i's. However, the lowest possible degree D in the degree isomorphism problem is 4 and $D_1 = D_2 = 2$. In fact, for the case of two polynomials f_1 and f_2 our results (and Kakié's) reduce to the classical

> *with $deg(a_1) < deg(f_2)$ and $deg(a_2) < deg(f_1)$, all polynomials of degree less than the degree of $f_1 f_2$ have unique representation $a_1 f_1 + a_2 f_2$.*

Our other approach to studying the lowest possible D in a degree isomorphism gives two lower bounds. The technique uses only the comparing of degrees and the equating of dimensions. One of the lower bounds obtained in this way is

$$D \;\geq\; \frac{\sum_{i=1}^{m} deg(f_i)}{m-1}.$$

We present examples to illustrate the concepts being discussed and to demonstrate optimality of various bounds.

In this paper we consider the degree isomorphism problem for relatively prime polynomials only. When g, the gcd of $f_1, \ldots, f_m$, is not a constant, the right-hand side of (1.1) must be replaced by $K^{(D)} \cdot g$. In this case, $D_1, \ldots, D_m$ and D give a degree isomorphism for $f_1, \ldots, f_m$ if and only if $D_1, \ldots, D_m$ and D give a degree isomorphism for $f_1/g, \ldots, f_m/g$. Therefore, we can obtain bounds for the general case by computing bounds for the special case and subtracting the degree of the gcd of $f_1, \ldots, f_m$.

2. Upper bound

Let R be a commutative ring with $K \subseteq R$ a field (R is a K-algebra) and I an ideal of R. Let $r \in R$. Suppose V is a vector subspace of R such that $R = V \oplus (I : r)$, where $(I : r) := \{a \in R \mid a \cdot r \in I\}$. The ideal generated by elements $f_1, \ldots, f_m \in R$ is denoted by $\langle f_1, \ldots, f_m \rangle$.

Lemma 2.1. *The map $\lambda : V \oplus I \longrightarrow R \cdot r + I$ defined by $\lambda(v, f) = v \cdot r + f$ is an isomorphism of vector spaces.*

Proof. The map

$$\gamma : R \longrightarrow \frac{R \cdot r + I}{I}$$

defined by $\gamma(a) = \overline{a \cdot r}$ has kernel $(I : r)$ by definition of $(I : r)$. This shows that γ carries V isomorphically to $(R \cdot r + I)/I$ and it immediately follows that λ is an isomorphism. □

LEMMA 2.2. *Let $\{f_1, \ldots, f_m\} \subset R$, I_0 any ideal and $I_i := I_0 + \langle f_1, \ldots, f_i \rangle$ for $i \in \{1, \ldots, m\}$. Suppose that V_i, for $i \in \{1, \ldots, m\}$, is a subspace of R such that $R = V_i \oplus (I_{i-1} : f_i)$.*

(a) The map

$$\lambda : I_0 \oplus V_1 \oplus \cdots \oplus V_m \longrightarrow I_m$$

defined by $\lambda(f, v_1, \ldots, v_m) = f + \sum_{i=1}^{m} v_i \cdot f_i$ is a vector space isomorphism.

(b) The map

$$\lambda' : V_1 \oplus \cdots \oplus V_m \longrightarrow \frac{I_m}{I_0}$$

defined by $\lambda'(v_1, \ldots, v_m) = \overline{\sum_{i=1}^{m} v_i \cdot f_i}$ is a vector space isomorphism.

(c) Let W be a vector subspace of I_m with $W \cap I_0 = \{0\}$ and $V_i \cdot f_i \subseteq W$ for each $i \in \{1, \ldots, m\}$. Then

$$\lambda'' : V_1 \oplus \cdots \oplus V_m \longrightarrow W$$

defined by $\lambda''(v_1, \ldots, v_m) = \sum_{i=1}^{m} v_i \cdot f_i$ is a vector space isomorphism.

PROOF. The proof of (a) immediately follows from the previous lemma by induction and (b) and (c) follow from (a). □

These results can be generalized to modules over non-commutative rings and abelian group complements instead of vector space complements.

In this paper we are interested in an application of the above results to the case $R = K[x]$. Let $f_1, \ldots, f_m$ be polynomials in $K[x]$ such that $\langle f_1, \ldots, f_m \rangle = K[x]$. For every $i \in \{2, \ldots, m\}$ let

$$G_i := deg(g_i), \quad \text{where } g_i \in K[x] \text{ is such that } \langle g_i \rangle = (\langle f_1, \ldots, f_{i-1} \rangle : f_i),$$

and

$$G_1 := \max_{2 \le i \le m} (G_i + deg(f_i)) - deg(f_1).$$

The following theorem provides a degree isomorphism with $D = \max_{2 \le i \le m}(G_i + deg(f_i))$ $= G_1 + deg(f_1)$ and hence provides an upper bound for this lowest possible D.

THEOREM 2.3. *The map*

$$\lambda : K^{(G_1)} \oplus \cdots \oplus K^{(G_m)} \longrightarrow K^{(\max_{2 \le i \le m}(G_i + deg(f_i)))}$$

defined by $\lambda(v_1, \ldots, v_m) = \sum_{i=1}^{m} v_i \cdot f_i$ is a vector space isomorphism.

PROOF. Let g be an arbitrary polynomial in $K[x]$ of degree G_1, $I_0 := \langle g \cdot f_1 \rangle$ and $W := K^{(G_1 + deg(f_1))}$. With these definitions, this theorem follows from Lemma 2.2(c). □

We briefly state the form of the above theorem when $f_1, \ldots, f_m$ are not relatively prime. Let g be the gcd of $f_1, \ldots, f_m$. With the G_i defined as above, the map

$$\lambda : K^{(G_1)} \oplus \cdots \oplus K^{(G_m)} \longrightarrow K^{(\max_{2 \le i \le m}(G_i + deg(f_i)) - deg(g))} \cdot g$$

defined by $\lambda(v_1, \ldots, v_m) = \sum_{i=1}^{m} v_i \cdot f_i$ is a vector space isomorphism.

Our only general upper bound follows directly from Theorem 2.3.

COROLLARY 2.4. *There exist polynomials $a_1, \ldots, a_m \in K[x]$ such that*

$$\sum_{i=1}^{m} a_i f_i = 1 \quad \textit{and} \quad deg(a_i) < G_i \textit{ for every } i \in \{1, \ldots, m\}.$$

In Kakié (1976) the following bound on the degrees of the a_i is given:

$$deg(a_i) \; < \; \max_{1 \le j \le m} (deg(f_j)) + \min_{1 \le j \le m} (deg(f_j)) - deg(f_i). \qquad (i = 1, \ldots, m)$$

If $m = 2$, the bound in Corollary 2.4 and Kakié's bound are equal. We prove in the following theorem that our bound is better for each of the a_i if no subset of cardinality 2 generates $K[x]$.

THEOREM 2.5. *Let $f_1, \ldots, f_m$ be ordered in such a way that*

$$deg(f_1) = \min_{1 \le j \le m} (deg(f_j))$$

and let T be a natural number such that no subset of the f_i of cardinality T is relatively prime. Then

$$G_1 \; \le \; \max_{1 \le j \le m} (deg(f_j)) - T + 1 \quad \textit{and} \quad G_i \; \le \; \min_{1 \le j \le m} (deg(f_j)) - T + 1 \;\; \textit{for } i \in \{2, \ldots, m\}.$$

PROOF. It follows from Theorem 2.3, viewing the range of λ as $K^{(G_1 + deg(f_1))}$, that

$$\sum_{i=2}^{m} G_i \; = \; deg(f_1).$$

By definition of T, at least T of $G_2, \ldots, G_m$ must be positive. Therefore,

$$G_i \; = \; deg(f_1) - \sum_{\substack{j \ne 1 \\ j \ne i}} G_j \; \le \; deg(f_1) - (T - 1). \qquad (i = 2, \ldots, m)$$

By definition of G_1,

$$G_1 \; = \; \max_{2 \le i \le m} (G_i + deg(f_i)) - deg(f_1) \; \le \; \max_{2 \le i \le m} (deg(f_i)) - T + 1. \;\; \square$$

3. Lower bounds

Suppose

$$\lambda : K^{(D_1)} \oplus \cdots \oplus K^{(D_m)} \longrightarrow K^{(D)},$$

defined by $\lambda(a_1, \ldots, a_m) = \sum_{i=1}^{m} a_i \cdot f_i$, is a vector space isomorphism. As $\lambda(\bigoplus_{j \ne i} K^{(D_j)})$ lies in the ideal $\langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m \rangle$, it follows that D_i must be greater than or equal to the degree of $gcd(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m)$. Since for every $i \in \{1, \ldots, m\}$

$$D \; \ge \; D_i + deg(f_i) \; \ge \; deg(gcd(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m)) + deg(f_i), \qquad (3.1)$$

we obtain the lower bound

$$D \;\geq\; \max_{1\leq i\leq m}(D_i + deg(f_i)) \;\geq\; \max_{1\leq i\leq m}(deg(gcd(f_1,\ldots,f_{i-1},f_{i+1},\ldots,f_m)) + deg(f_i)). \tag{3.2}$$

Since

$$\sum_{i=1}^{m} D_i \;=\; D$$

we can sum the m inequalities $D \geq D_i + deg(f_i)$ in (3.1) and get the bound

$$D \;\geq \frac{\sum_{i=1}^{m} deg(f_i)}{m-1}. \tag{3.3}$$

Example 3.1. Let q_1, q_2, q_3 be linear polynomials and d_1, d_2, d_3 polynomials of degree 2. We assume that these 6 polynomials are pairwise relatively prime and that d_1, d_2, d_3 are K-linearly independent. Let

$$f_1 := q_2 \cdot q_3 \cdot d_1, \qquad f_2 := q_1 \cdot q_3 \cdot d_2, \qquad f_3 := q_1 \cdot q_2 \cdot d_3.$$

Then

$$\lambda : K^{(2)} \oplus K^{(2)} \oplus K^{(2)} \longrightarrow K^{(6)}$$

defined by $\lambda(a_1, a_2, a_3) = \sum_{i=1}^{3} a_i \cdot f_i$ is a vector space isomorphism. In this case bound (3.3) is attained and is strictly greater than bound (3.2).

Example 3.2. Let q_1, q_2, q_3 be linear polynomials and d a polynomial of degree 2. We assume that these 4 polynomials are pairwise relatively prime. Let

$$f_1 := q_2 \cdot q_3, \qquad f_2 := q_1 \cdot q_3, \qquad f_3 := q_1 \cdot q_2 \cdot d.$$

Then, by Theorem 2.3,

$$\lambda : K^{(3)} \oplus K^{(1)} \oplus K^{(1)} \longrightarrow K^{(5)}$$

defined by $\lambda(a_1, a_2, a_3) = \sum_{i=1}^{3} a_i \cdot f_i$ is a vector space isomorphism. In this case bound (3.2) is attained and is strictly greater than bound (3.3).

4. A closer analysis

Not surprisingly, the ideals generated by all but one of the f_i play a significant role in a finer analysis. This finer analysis naturally ties in to the method of partial fractions. For $i \in \{1,\ldots,m\}$ define $q_i := gcd(f_1,\ldots,f_{i-1},f_{i+1},\ldots,f_m)$. Since $\langle f_1,\ldots,f_m\rangle = K[x]$, the polynomials $q_1,\ldots,q_m$ are pairwise relatively prime. Therefore, $q_1\cdots q_{i-1}\cdot q_{i+1}\cdots q_m$ divides f_i. Let

$$d_i := \frac{f_i}{q_1\cdots q_{i-1}\cdot q_{i+1}\cdots q_m}.$$

Lemma 4.1. *Let $i \in \{2,\ldots,m\}$. The ideal $(\langle f_1,\ldots,f_{i-1}\rangle : f_i)$ is generated by the polynomial*

$$\frac{q_i \cdot gcd(d_1,\ldots,d_{i-1})}{gcd(d_1,\ldots,d_{i-1},d_i)}.$$

PROOF. Since $\langle f_1, \ldots, f_m \rangle = K[x]$, q_j and d_j are relatively prime as are f_j and q_j for every $j \in \{1, \ldots, m\}$. Therefore, the ideal $\langle f_1, \ldots, f_{i-1} \rangle$ is generated by

$$gcd(d_1, \ldots, d_{i-1}) \cdot \prod_{j=i}^{m} q_j$$

and the ideal $(\langle f_1, \ldots, f_{i-1} \rangle : f_i)$ is generated by

$$\frac{q_i \cdot gcd(d_1, \ldots, d_{i-1})}{gcd(d_1, \ldots, d_{i-1}, d_i)}. \quad \square$$

Let $Q := \sum_{i=1}^{m} deg(q_i)$. With this Q, the bound (3.2) becomes

$$D \;\geq\; Q + \max_{1 \leq i \leq m} (deg(d_i)). \tag{4.1}$$

The following proposition shows that this lower bound is achieved if one of the d_i is of degree zero. In this case we have found the lowest possible D for the degree isomorphism problem.

PROPOSITION 4.2. *Suppose that there exists a $j \in \{1, \ldots, m\}$ such that d_j is of degree zero. Then*

$$Q + \max_{1 \leq i \leq m} (deg(d_i))$$

is the lowest possible D for the degree isomorphism problem.

PROOF. Without loss of generality assume that d_1 is of degree zero. Then we obtain from Lemma 4.1 that

$$G_i \;=\; deg(gcd(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m)) \qquad (i = 2, \ldots, m) \tag{4.2}$$

and

$$G_1 \;=\; deg(gcd(f_2, f_3, \ldots, f_m)) + \max_{2 \leq j \leq m} (deg(d_j)). \tag{4.3}$$

Adding all the G_i's gives

$$\sum_{i=1}^{m} G_i \;=\; Q + \max_{2 \leq i \leq m} (deg(d_i)). \tag{4.4}$$

Since d_1 is of degree zero the max in (4.4) can actually be taken over $1 \leq i \leq m$. Therefore, it follows from Theorem 2.3 and (4.1) that $Q + \max_{1 \leq i \leq m}(deg(d_i))$ is the lowest possible D for the degree isomorphism problem. $\square$

THEOREM 4.3. (PARTIAL FRACTIONS THEOREM) *All the d_i are of degree zero if and only if Q is the lowest possible D in the degree isomorphism problem.*

PROOF. By (4.1) if Q is the lowest possible D then all d_i must have degree zero. Conversely, if all the d_i are of degree zero then by the preceding proposition Q is the lowest possible D. $\square$

Theorem 4.3 is called the "Partial Fractions Theorem" because Q being the lowest possible D is equivalent to:

> *Let $q := q_1 \cdots q_m$. For every polynomial of degree lower than q the rational function b/q has a unique representation $\sum a_i/q_i$, where each a_i is of lower degree than q_i.*

References

Kakié, K. (1976). The resultant of several homogeneous polynomials in two indeterminates. *Proc. AMS* **54**, 1–7.

Shiffman, B. (1989). Degree bounds for the division problem in polynomial ideals. *Michigan Math. J.* **36**, 163–171.