SIGSAM Bulletin, vol. 27, nr. 4, p. 2 (1993).

Direct Proof of a Theorem by Kalkbrener, Sweedler, and Taylor*

Erich Kaltofen

Department of Computer Science, Rensselaer Polytechnic Institute
Troy, New York 12180-3590; Inter-Net: `kaltofen@cs.rpi.edu`

For given $f_1, \ldots, f_m \in K[x]$ that are relatively prime, where K is a field, Kalkbrener, Sweedler, and Taylor (1993) present degree bounds on the a_i needed to express 1 (and other low degree polynomials) as $\sum a_i f_i$. Their bounds are an improvement on bounds given by Kakié (1976). This note presents a direct proof of the following fact.

Theorem: *Let $f_1, \ldots, f_m$ be $m \geq 2$ polynomials in $K[x]$ without a common polynomial divisor such that $\deg(f_1) \leq \deg(f_i)$ for all $2 \leq i \leq m$. Suppose that every subset of T polynomials $f_1, f_{i_2}, \ldots, f_{i_T}$ has a common polynomial divisor, where $2 \leq i_2 < i_3 < \cdots < i_T \leq m$. Then there exist polynomials $a_1, \ldots, a_m \in K[x]$ such that $a_1 f_1 + \cdots + a_m f_1 = 1$ and $\deg(a_1) \leq \max_{2\leq j\leq m}\{\deg(f_j)\} - (T-1)$ and $\deg(a_i) \leq \deg(f_1) - (T-1)$ for all $i \geq 2$.*

Note that the above theorem is slightly stronger than the one presented in Kalkbrener et al., where T is taken so that no arbitrary subset of $\{f_1, \ldots, f_m\}$ of cardinality T is relatively prime. However, the restriction to subsets containing f_1 can also be incorporated in Kalkbrener's et al. argument (see the proof of their Theorem 2.5).

My arguments are based on the technique used to prove the uniqueness of the partial fraction decomposition of a rational function, whereas Kalkbrener et al. use isomorphisms on the vectorspaces generated by degree bounded polynomials and their direct products.

Proof: Without loss of generality one may assume that for all $i \geq 2$ we have

$$g_i = \mathrm{GCD}(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m) \neq 1. \qquad (1)$$

Otherwise, pick a relatively prime subset containing f_1. Let $G = g_2 \cdots g_m$. Therefore

$$f_1 = G \cdot f_1', \qquad f_i = G/g_i \cdot f_i' \quad i \geq 2.$$

where $\mathrm{GCD}(g_i, f_i) = 1$ and $\mathrm{GCD}(g_i, g_j) = 1$ for $i \neq j$, because the set of all f_i is relatively prime. We prove by induction on m that for a set of polynomials satisfying (1) and any polynomial h there exist polynomials $a_1, \ldots, a_m$ such that

$$a_1 f_1 + \cdots + a_m f_m = h \qquad (2.1)$$

and

$$\deg(a_i) < \deg(f_1) - (m-2) \quad \text{for} \quad i \geq 2. \qquad (2.2)$$

Note that $\deg(g_m) \leq \deg(f_1) - (m-2)$, since the g_i are non-constant. For $m = 2$, the scheme $a_1' f_1 + a_2' f_2 = 1$ with a_1' and $a_2' \in K[x]$ leads to the solution $a_1 = h a_1' + q_2 f_2$ and $a_2 = r_2$ where $a_2' h = q_2 f_1 + r_1$ with $\deg(r_1) < \deg(f_1)$. Hence for general m there are polynomials A and a_m such that

$$A g_m + a_m f_m = h$$

where $\deg(a_m) < \deg(g_m)$. It remains to write

$$A = a_1(f_1/g_m) + \cdots + a_{m-1}(f_{m-1}/g_m)$$

with $\deg(a_i) < \deg(f_1/g_m) - (m-3) \leq \deg(f_1) - (m-2)$ for $i \geq 2$. Note that the set $f_1/g_m, \ldots f_{m-1}/g_m$ satisfies condition (1) for possibly new non-constant GCDs that must be divisible by the old g_i. This establishes (2.1) and (2.2). The bound for a_1 follows from $a_1 = (1 - a_2 f_2 - \cdots - a_m f_m)/f_1$.

Acknowledgement: Thanks to Michael Kalkbrener for pointing out a problem with my earlier argument.

Literature Cited

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

Kalkbrener, M., Sweedler, M., and Taylor, L., "Low degree solutions to linear equations with $K[x]$ coefficients," *J. Symbolic Comput.* **16**/1, pp. 75–81 (1993).

*This material is based on work supported in part by the National Science Foundation under Grant No. CCR-90-06077.