THE DISTRIBUTION OF SOLUTIONS OF CONGRUENCES: *CORRIGENDUM AND ADDENDUM*

J. H. H. CHALK AND K. S. WILLIAMS

The reviewer [*Math. Reviews*, **32** (1966), 7526] has stated that he could not follow case (iii) of the proof* of Lemma 7 and upon examination we find that the argument is incomplete (on p. 183, the degree of d_1 may not be smaller than that of g). The following version of the proof (which is given with full details), circumvents the difficulty and has been designed to show, further, that the constant implied in the O-symbol is independent of the number of variables. This minor refinement may be of some interest as the corresponding estimates of Lang and Weil [*Amer. J. Math.*, **76** (1954), 819–827; *cf.*, Lemmas 1, 2 and Theorem 1] for general varieties over a finite field lack this feature. Throughout, we use the symbol $\deg F$ to denote the total degree of an element F of a polynomial domain $k[\underline{x}]$, where $k = [p]$ is the field of residue classes mod p and $\underline{x} = (x_1, x_2, \ldots, x_n)$. $N_r(\dagger)$ will denote the number of r-tuples $(x_{n-r+1}, \ldots, x_n) \in k^r$ with some specific property $\dagger$. We prove that, if $n \geqslant 1$ and f, g are elements of $k[\underline{x}]$ with no non-constant common factor in $k[\underline{x}]$, i.e. $(f, g)_p = 1$, then

$$N_n(f = g = 0) = O_d(p^{n-2}), \tag{1}$$

where the constant in the O-symbol depends only upon $d = \max(\deg f, \deg g)$. The argument is entirely elementary and uses a method of descent in which the number of variables n and the minimum degree, defined by

$$c(f, g) = \min(\deg f, \deg g),$$

are simultaneously diminished at each step of the descent. It makes use of a corresponding (trivial) estimate for the case of one polynomial, i.e. if $F \in k[\underline{x}] - 0$ and $\partial = \deg F$, then $N_n(F = 0) = O_\partial(p^{n-1})$. Thus, if f, g are disjoint in the sense that $f \in k[x_1, \ldots, x_r]$, $g \in k[x_{r+1}, \ldots, x_n]$ after a suitable permutation of $x_1, \ldots, x_n$, then $(f, g)_p = 1$ implies that

$$N_n(f = g = 0) = \begin{cases} O_d(p^{r-1}p^{n-r-1}) = O_d(p^{n-2}), & \text{if } f \notin k,\ g \notin k, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

We note also that it is sufficient to establish (1) for a pair $\mathfrak{p}$, $\mathfrak{q}$ of *irreducible* polynomials in $k[\underline{x}]$ with $(\mathfrak{p}, \mathfrak{q})_p = 1$, since

$$N_n(f = g = 0) \leqslant \sum_{\mathfrak{p} | f,\, \mathfrak{q} | g} N_n(\mathfrak{p} = \mathfrak{q} = 0), \tag{3}$$

where $\mathfrak{p}$, $\mathfrak{q}$ are the irreducible factors in $k[\underline{x}]$ of f, g respectively,

$$\max(\deg \mathfrak{p}, \deg \mathfrak{q}) \leqslant d,$$

the number of terms in the sum is $O_d(1)$ and $(\mathfrak{p}, \mathfrak{q})_p = 1$. Thus, let $\mathfrak{p}, \mathfrak{q}$ be given irreducible polynomials in $k[\underline{x}]$ with $(\mathfrak{p}, \mathfrak{q})_p = 1$, $\delta = \max(\deg \mathfrak{p}, \deg \mathfrak{q})$. If necessary, permute $\mathfrak{p}$, $\mathfrak{q}$ to arrange that

$$c(\mathfrak{p}, \mathfrak{q}) = \deg \mathfrak{p} \leqslant \deg \mathfrak{q} = \delta.$$

* *Mathematika*, 12 (1965), 176–192.

If $\mathfrak{p}$, $\mathfrak{q}$ are disjoint then the estimate in (2) gives the required result immediately. If not, we apply the following process. Permute $x_1, \ldots, x_n$ to ensure that both $\mathfrak{p}$ and $\mathfrak{q}$ belong to $k[\underline{x}] - k[\underline{x}']$, where $\underline{x}' = (x_2, \ldots, x_n)$. Then, since $(\mathfrak{p}, \mathfrak{q})_p = 1$, the resultant Ω of $\mathfrak{p}$ and $\mathfrak{q}$ (regarded now as polynomials in x_1), satisfies

$$\Omega \in k[\underline{x}'] - 0, \quad \deg \Omega \leqslant 2\delta, \tag{4}$$

and

$$a\mathfrak{p} + b\mathfrak{q} = \Omega, \tag{5}$$

for suitable elements a, b of $k[\underline{x}]$. Each irreducible factor $\mathfrak{r}$ of Ω has the property $(\mathfrak{p}, \mathfrak{r})_p = 1$, since $\mathfrak{r} \in k[\underline{x}']$, $\mathfrak{p} \notin k[\underline{x}']$ and $\mathfrak{p}$ is irreducible in $k[\underline{x}]$. Hence

$$\begin{aligned} N_n(\mathfrak{p} = \mathfrak{q} = 0) &\leqslant N_n(\mathfrak{p} = \Omega = 0) \\ &\leqslant \sum_{\mathfrak{r}|\Omega} N_n(\mathfrak{p} = \mathfrak{r} = 0), \end{aligned} \tag{6}$$

by (5), and

$$c(\mathfrak{p}, \mathfrak{r}) \leqslant \deg \mathfrak{p} = c(\mathfrak{p}, \mathfrak{q}). \tag{7}$$

Note that the number of terms in the sum over $\mathfrak{r}$ in (6) is bounded by $\deg \Omega \leqslant 2\delta$. As $\mathfrak{p} \notin k[\underline{x}']$, it is expressible in the form

$$\mathfrak{p} = a_0(\underline{x}')\, x_1^{\,e} + \ldots + a_{e-1}(\underline{x}')\, x_1 + a_e(\underline{x}'),$$

where $1 \leqslant e \leqslant \delta$ and $a_0(\underline{x}')$ is not identically 0. Then, for each irreducible $\mathfrak{r}|\Omega$ we consider two cases according as $\mathfrak{r}|a_i$ $(i = 0, 1, \ldots, e-1)$ or $\mathfrak{r} \nmid a_i$ for some $i < e$:

(i) $\mathfrak{r}|a_i$ $(0 \leqslant i \leqslant e-1)$. Then $(\mathfrak{p}, \mathfrak{r})_p = 1$ implies that $(a_e, \mathfrak{r})_p = 1$ and so

$$N_n(\mathfrak{p} = \mathfrak{r} = 0) = pN_{n-1}(a_e = \mathfrak{r} = 0).$$

Also, since $\mathfrak{r}|a_0$ and a_0 is not identically 0, $(e \geqslant 1)$,

$$\deg \mathfrak{r} \leqslant \deg a_0 < \deg \mathfrak{p},$$

whence

$$c(a_e, \mathfrak{r}) \leqslant c(\mathfrak{p}, \mathfrak{r}) < \deg \mathfrak{p} = c(\mathfrak{p}, \mathfrak{q}).$$

(ii) $\mathfrak{r} \nmid a_j$, where $j < e$. Define the following sets

$$\begin{aligned} E &= \{\underline{x}' \in k^{n-1} | \mathfrak{r} = 0\}, \\ E_1 &= \{\underline{x}' \in E | a_0 = \ldots = a_{e-1} = 0\}, \\ E_2 &= \{\underline{x}' \in E | a_0, \ldots, a_{e-1} \text{ not all } 0\}, \end{aligned}$$

where $E_1 \cup E_2 = E$, $E_1 \cap E_2 = \emptyset$. Then

$$\begin{aligned} |E_1| &\leqslant N_{n-1}(a_j = \mathfrak{r} = 0), \\ |E_2| &\leqslant |E| = O_\delta(p^{n-2}). \end{aligned}$$

Hence

$$N_n(\mathfrak{p} = \mathfrak{r} = 0,\ \underline{x}' \in E_1) \leqslant p|E_1| \leqslant pN_{n-1}(a_j = \mathfrak{r} = 0),$$

and

$$N_n(\mathfrak{p} = \mathfrak{r} = 0,\ \underline{x}' \in E_2) \leqslant e|E_2| = O_\delta(p^{n-2});$$

whence

$$\begin{aligned} N_n(\mathfrak{p} = \mathfrak{r} = 0) &= N_n(\mathfrak{p} = \mathfrak{r} = 0,\ \underline{x}' \in E) \\ &= N_n(\mathfrak{p} = \mathfrak{r} = 0,\ \underline{x}' \in E_1) + N_n(\mathfrak{p} = \mathfrak{r} = 0,\ \underline{x}' \in E_2), \\ &\leqslant pN_{n-1}(a_j = \mathfrak{r} = 0) + O_\delta(p^{n-2}). \end{aligned}$$

Note also that $j < e$ implies that $\deg a_j < \deg \mathfrak{p}$, and so

$$c(a_j, \mathfrak{r}) < \deg \mathfrak{p} = c(\mathfrak{p}, \mathfrak{q}).$$

Thus, combining (i) and (ii), we have for each irreducible $\mathfrak{r}|\Omega$,

$$N_n(\mathfrak{p} = \mathfrak{r} = 0) \leqslant pN_{n-1}(a_i = \mathfrak{r} = 0) + O_\delta(p^{n-2}), \quad \text{for some } i, \tag{8}$$

where

$$\max(\deg a_i, \deg \mathfrak{r}) \leqslant 2\delta, \quad c(a_i, \mathfrak{r}) < c(\mathfrak{p}, \mathfrak{q}), \quad (a_i, \mathfrak{r})_p = 1. \tag{9}$$

For the irreducible factors $\mathfrak{s}$ of each such a_i, we write

$$N_{n-1}(a_i = \mathfrak{r} = 0) \leqslant \sum_{\mathfrak{s}|a_i} N_{n-1}(\mathfrak{r} = \mathfrak{s} = 0); \tag{10}$$

then, from (6), (7), (8), (9), and (10), we see that $N_n(\mathfrak{p} = \mathfrak{q} = 0)$ is bounded above by a sum of $O_\delta(1)$ terms of the form

$$pN_{n-1}(\mathfrak{r} = \mathfrak{s} = 0) + O_\delta(p^{n-2}),$$

where each such pair $\mathfrak{r}$, $\mathfrak{s}$ of irreducible polynomials in $k[\underline{x}']$ satisfies

$$\max(\deg \mathfrak{r}, \deg \mathfrak{s}) \leqslant 2\delta, \quad c(\mathfrak{r}, \mathfrak{s}) < c(\mathfrak{p}, \mathfrak{q}), \quad (\mathfrak{r}, \mathfrak{s})_p = 1. \tag{11}$$

If each of the new pairs $\mathfrak{r}$, $\mathfrak{s}$ is disjoint the process stops. Otherwise, we apply the process again to all pairs $\mathfrak{r}$, $\mathfrak{s}$ which are not disjoint, producing $O_\delta(1)$ pairs u, v in $k[\underline{x}'']$, with $\underline{x}'' = (x_3, \ldots, x_n)$, $(u, v)_p = 1$, $c(u, v) < c(\mathfrak{r}, \mathfrak{s})$, (for some pair $\mathfrak{r}$, $\mathfrak{s}$), $\max(\deg u, \deg v) \leqslant 4\delta$, which contribute an additional $O_\delta(1)$ terms of the form

$$p\big(pN_{n-2}(u = v = 0) + O_\delta(p^{n-3})\big) = p^2 N_{n-2}(u = v = 0) + O_\delta(p^{n-2})$$

to $N_n(\mathfrak{p} = \mathfrak{q} = 0)$. Clearly, the process can be repeated as long as there is at least one pair which is not disjoint. Note that the number of possible repetitions of the process is not only bounded by n but, in view of the strict inequality in (11), it is also bounded by $c(\mathfrak{p}, \mathfrak{q}) \leqslant \delta$. Thus ultimately, the set of $O_\delta(1)$ pairs so produced will consist entirely of disjoint pairs, each contributing a term of the form $p^\nu N_{n-\nu} + O_\delta(p^{n-2})$, for some ν with $1 \leqslant \nu \leqslant \delta$, to $N(\mathfrak{p}, \mathfrak{q} = 0)$. By replacing n by $n - \nu$ in (2), we see that each such $N_{n-\nu}$ is bounded by $O_\delta(p^{n-\nu-2})$ and this completes the proof.

University of Toronto
and
Carleton University.

(*Received on the 24th of July*, 1968.)

Printed by C. F. Hodgson & Son, Ltd., 23 Pakenham Street, London, W.C.1