2-Adic zeros of diagonal forms

Michael P. Knapp

Department of Mathematics and Statistics
Loyola University Maryland
4501 North Charles Street
Baltimore, MD 21210-2699
USA

Abstract

Consider an additive form $F(\mathbf{x}) = a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d$ whose coefficients are 2-adic integers. In this article we give an exact formula, in terms of d, for the smallest number of variables which guarantees that F has a nontrivial zero in the 2-adic integers regardless of the values of the coefficients.

Keywords: diagonal forms, Artin's conjecture, 2-adic solubility
2000 MSC: 11D72 (primary), 11D88 (secondary)

1. Introduction

In this article, we study conditions under which diagonal forms have nontrivial 2-adic zeros. Suppose that $F(\mathbf{x})$ is a polynomial of the form

$$F(\mathbf{x}) = a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d \tag{1}$$

with all coefficients in the field $\mathbb{Q}_2$ of 2-adic numbers. We wish to find a condition on the number of variables which guarantees that regardless of the coefficients, the equation $F(\mathbf{x}) = 0$ has a solution where all of the variables are in $\mathbb{Q}_2$ and at least one variable is nonzero.

One of the earliest results about additive forms over p-adic fields was due to Brauer [1], who showed that if the coefficients of F in (1) are *rational* integers, then given the degree d of the form, there exists a number $\Gamma^*(d)$ such that if $s \geq \Gamma^*(d)$, then the form $F(\mathbf{x})$ has nontrivial zeros in p-adic integers for all primes p, regardless of the coefficients of F. Brauer's result is actually stronger than this, as it applies to systems of forms, and the forms are only

Email address: mpknapp@loyola.edu (Michael P. Knapp)

required to be homogeneous, not necessarily additive. However, Brauer's paper does not give either a formula or an upper bound for $\Gamma^*(d)$.

The first quantitative result in this direction was by Davenport & Lewis [2], who showed that $\Gamma^*(d) \le d^2 + 1$ and that equality holds whenever $d+1$ is prime. Other results along these lines for either single forms or systems of forms have been given by Brüdern & Godinho [3, 4], Davenport & Lewis [5, 6], Dodson [7, 8], Knapp [9, 10], Low, Pitman & Wolff [11], and Wooley [12], among others. The majority of results of this type have been proven by first fixing the prime p and finding an upper bound for $\Gamma_p^*(d)$, which is defined in the same way as $\Gamma^*(d)$ except that one only considers p-adic solubility for the specified prime, and allows the coefficients to be any p-adic integers. (It turns out that for a specified prime p, the situation with rational integral coefficients and the situation with p-adic integral coefficients are equivalent, so there is no loss here. The coefficients were only originally restricted to be rational integers so that the equation would be defined over all of the fields $\mathbb{Q}_p$.) Once the bound for $\Gamma_p^*(d)$ is established, one can find the maximum of this bound over all primes, obtaining a bound on $\Gamma^*(d)$. Given this method, it seems natural to study the functions $\Gamma_p^*(d)$ for specific values of p, and in this article we focus our attention on the situation when $p = 2$.

When calculating values of $\Gamma^*(d)$, one finds that they are very irregular. For example, we have $\Gamma^*(6) = 37$ [2], $\Gamma^*(7) = 22$ [7, 13, 14, all independently], $\Gamma^*(8) = 39$ [15], $\Gamma^*(9) = 37$ [7, 14, independently], and $\Gamma^*(10) = 101$ [2]. In fact, no explicit formula is known which gives the value of $\Gamma^*(d)$ for all values of d. Therefore it is perhaps surprising that it is possible to give an explicit formula which yields the exact value of $\Gamma_2^*(d)$ for all degrees d.

Theorem 1.1. *Write $d = 2^\tau d_0$, where d_0 is an odd integer, and define the number γ by*

$$\gamma = \gamma(d) = \begin{cases} 1 & \text{if } \tau = 0; \\ \tau + 2 & \text{if } \tau > 0. \end{cases}$$

Further, write $d = \gamma q + r$, where q and r are integers with $0 \le r \le \gamma - 1$. Then we have

$$\Gamma_2^*(d) = \begin{cases} 5 & \text{if } d = 2; \\ (2^\gamma - 1)\, q + 2^r & \text{otherwise.} \end{cases}$$

It is not hard to show that $\Gamma_2^*(d)$ must be at least as large as the bound in the theorem. Suppose first that $d \neq 2$. By the theory of d-th power residues modulo powers of 2, one can see that if $2 \nmid x$, then $x^d \equiv 1 \pmod{2^\gamma}$. Consider the form

$$F = \sum_{i=1}^{2^\gamma - 1} x_i^d + 2^\gamma \cdot \sum_{i=(2^\gamma-1)+1}^{2\cdot(2^\gamma-1)} x_i^d + \cdots$$
$$+ 2^{(q-1)\gamma} \cdot \sum_{i=(q-1)(2^\gamma-1)+1}^{q(2^\gamma-1)} x_i^d + 2^{q\gamma} \cdot \sum_{i=q(2^\gamma-1)+1}^{q(2^\gamma-1)+2^r-1} x_i^d.$$

Since there are only $2^\gamma - 1$ variables with coefficients not divisible by 2^γ, the only way to have $F \equiv 0 \pmod{2^\gamma}$ is to have each of $x_0, \ldots, x_{2^\gamma-1}$ divisible by 2. Similarly, one can see that in any nontrivial 2-adic zero, all of the variables must be divisible by 2. Because the form is homogeneous, we could get another zero by dividing each variable by 2. Doing this repeatedly would eventually lead to a 2-adic integral solution with at least one variable not divisible by 2, yielding a contradiction.

If $d = 2$, then we can show that $\Gamma_2^*(2) \geq 5$ by noting that the congruence $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod 8$ has no solutions with any of the x_i odd. In the same way as above, we can then show that the equation $x_1^2+x_2^2+x_3^2+x_4^2 = 0$ has no nontrivial 2-adic integral solutions. Moreover, since it is well-known that $\Gamma^*(2) = 5$ (for example since $2+1$ is prime), we must have $\Gamma_2^*(2) \leq 5$. Together, these inequalities show that $\Gamma_2^*(2) = 5$. When we consider Theorem 1.1 in the remainder of this article, we will assume that $d \neq 2$.

As an interesting consequence of this theorem, we have the following corollary.

Corollary 1.2. *We have* $\Gamma^*(32) = 524$.

This is immediate from results in [16]. In that article, we show that $\Gamma_p^*(32) \leq 513$ for all $p > 2$. Since Theorem 1.1 gives $\Gamma_2^*(32) = 524$, this completes the proof.

It is interesting to note in this corollary that we have $\Gamma^*(32) \not\equiv 1 \pmod{32}$. For almost all of the known values of $\Gamma^*(d)$, it is the case that $\Gamma^*(d) \equiv 1$

(mod d), and it had been conjectured at one point that this congruence must hold for all d. Bovey [15] disproved this when he showed that $\Gamma^*(8) = 39$. This example is only the second known value of d for which the congruence fails.[1]

Before ending this section, we mention that the techniques used in the proof can be used to prove a theorem in the field of graph pebbling. Suppose that G is a directed cycle graph with n vertices such that all of the edges point clockwise, and that a positive integer $d < n$ is given. Using the techniques in this article, we can determine the minimal number s such that if s pebbles are placed on the graph, in any configuration, then there is a sequence of pebbling moves which moves a pebble at least d vertices away from where it started. In fact, the bound itself is entirely analogous to the bound in this article. The interested reader may refer to [18], which may be thought of as a companion paper to this one, for details.

2. Contractions

In this section, we define the notion of a contraction, which will be useful when proving Theorem 1.1. First, we note that in (1), we can write

$$F = F_0 + 2F_1 + 2^2F_2 + 2^3F_3 + \cdots ,$$

where each variable in each of the forms $F_0, F_1, \ldots$ has a coefficient not divisible by 2 and each variable in F is in exactly one of the F_i. If a variable x is included in the form F_i, then we say that x is at **level** i in F. Further, if $i \geq d$, then by making a change of variables of the form $x' = 2x$, we can lower the level of x to $i - d$. Moreover, the form that results from making this change of variables has nontrivial 2-adic integral zeros if and only if F does. Hence we may assume without loss of generality that every variable in F has level at most $d - 1$.

We can now define contractions of variables. Suppose that F is as in (1), that we have some variables in F, say $x_1, \ldots, x_t$ for example, and that these

[1] In unpublished work, Jessica Jennings (an undergraduate student at Loyola University Maryland at the time) has shown that $\Gamma^*(54) = 1049$, giving a third example. This example was recently discovered independently by Diane Soares Veras in her Ph.D. thesis [17].

variables are at (possibly different) levels at most $j-1$. Suppose further that we can find numbers $b_1, \ldots, b_t$ such that

$$a_1 b_1^d + \cdots + a_t b_t^d = 2^j m,$$

with m odd. Then setting $x_i = b_i T$ for $1 \leq i \leq t$ yields a new variable T at level j with coefficient $2^j m$. This operation is called a **contraction of variables to a new variable at level j**.

Along with contractions, our main tool for finding nontrivial 2-adic zeros of (1) is the following version of Hensel's Lemma.

Lemma 2.1. *Let F be a form as in (1). Write $d = 2^\tau d_0$, with d_0 odd, and let γ be defined as in the statement of Theorem 1.1. Suppose that for some positive integer n, we can find a vector $\mathbf{z}$ such that*

$$F(\mathbf{z}) \equiv 0 \pmod{p^{n+\gamma}} \tag{2}$$

and at least one variable at level n or below is odd. Then $\mathbf{z}$ can be lifted to a nontrivial 2-adic integral zero of (1).

Combining our tools, suppose that for some n we can use contractions to construct a variable T at level $n+\gamma$ or higher, and that in these contractions we use a variable that was originally at level n. Then by setting $T = 1$ and setting any variables not involved in the contractions equal to 0, the condition (2) is satisfied, and Lemma 2.1 may be applied. Therefore, our goal in the proof is to show that we can "move" a variable up at least γ levels by using contractions.

3. Preliminaries

In this section, we give the preliminary lemmata needed to prove our formula for the value of $\Gamma_2^*(d)$. We begin with two straightforward lemmata which we will need to bound the number of variables at different levels.

Lemma 3.1. *Suppose that d, N, and a are positive integers such that $N/d > 2^1 - 1 = 1$ and $aN/d > 2^a - 1$. Then we must also have $kN/d > 2^k - 1$ whenever $2 \leq k \leq a-1$.*

Proof. Let $f(k) = \frac{N}{d}k - 2^k + 1$. Then the lemma is true if we can prove that $f(k) > 0$ for $1 \le k \le a$. By hypothesis, this is true for $k = 1$ and $k = a$. Considering k as a real variable, we have $f'(k) = \frac{N}{d} - 2^k \ln 2$. Clearly there is only one point $k = k^*$ such that $f'(k) = 0$. Moreover, we have $f'(k) > 0$ for $k < k^*$ and $f'(k) < 0$ for $k > k^*$. This implies that once $f(k)$ begins decreasing, it can never increase again. If we were to have $f(k) \le 0$ for some k between 1 and a, then $f(k)$ would have to decrease after $k = 1$ and then start increasing again to yield $f(a) > 0$. But this cannot happen. This completes the proof of the lemma.

□

Lemma 3.2. *Suppose that γ, q are positive integers with $\gamma \ge 3$, that r is an integer with $0 \le r < \gamma$, and set $d = \gamma q + r$. Moreover, suppose that $m_0, \dots, m_{\gamma-2}$ are integers such that*

$$m_0 + \cdots + m_{k-1} \ge \frac{k\left((2^\gamma - 1)q + 2^r\right)}{d}$$

for $1 \le k \le \gamma - 1$. Then we have

$$m_0 + \cdots + m_{k-1} > 2^k - 1$$

for $1 \le k \le \gamma - 1$.

Proof. By Lemma 3.1 with $N = (2^\gamma - 1)q + 2^r$, it suffices to prove the conclusion for $k = 1$ and $k = \gamma - 1$. When $k = 1$, our hypothesis is that

$$m_0 \ge \frac{(2^\gamma - 1)q + 2^r}{\gamma q + r}.$$

To see that this is greater than 1, we simply note that $2^\gamma - 1 \ge \gamma$ and $2^r > r$ for all nonnegative integers γ and r. When $k = \gamma - 1$, we need to show that

$$\frac{(\gamma - 1)\left((2^\gamma - 1)q + 2^r\right)}{d} > 2^{\gamma-1} - 1.$$

Some algebra shows that this is true if and only if we have

$$2^{\gamma-1}(\gamma q - 2q - r) + (2^r(\gamma - 1) + q + r) > 0. \tag{3}$$

Clearly, the number $2^r(\gamma - 1) + q + r$ is positive. Moreover, the number $\gamma q - 2q - r$ is nonnegative whenever $r \le (\gamma - 2)q$. If this is true, then (3) is also true. Therefore, since we must have $r \leq \gamma - 1$, the inequality (3) can only potentially fail to hold when $(\gamma - 2)q < r \leq \gamma - 1$, which implies that $q < 1 + \frac{1}{\gamma - 2}$. Hence the only potential problems arise when $q = 1$, in which case we must have $r = \gamma - 1$. In this case, (3) becomes

$$2^{\gamma-1}(\gamma - 2) + \gamma > 0,$$

which is clearly true since $\gamma \geq 3$. This completes the proof of the lemma.

□

Another key tool in the proof is the following combinatorial lemma due to Davenport & Lewis [2].

Lemma 3.3. *Let $a_0, a_1, \ldots, a_{d-1}$ be real numbers, and put $a_{j+d} = a_j$ for all j. Let*

$$a_0 + a_1 + \cdots + a_{d-1} = s.$$

Then there exists a number r such that

$$a_r + \cdots + a_{r+t-1} \geq ts/d \qquad \textit{for} \qquad t = 1, \ldots, d.$$

The next lemma is a special case of a lemma due to Davenport & Lewis [2], and shows that it suffices to study additive forms with certain additional properties. Part of this lemma formalizes our remarks at the beginning of Section 2, and part is a corollary of Lemma 3.3.

Lemma 3.4. *By a nonsingular change of variables of the form $x_i = l_i x_i'$, any additive form as in (1) can be transformed into one of the type*

$$F = F_0 + 2F_1 + \cdots + 2^{d-1}F_{d-1},$$

where each F_i is an additive form in m_i variables, and the variables in each F_i are distinct. Moreover, each variable in each F_i appears with a coefficient which is nonzero modulo 2, and for $1 \leq i \leq d$, we have

$$m_0 + m_1 + \cdots + m_{i-1} \geq is/d.$$

Since making a nonsingular change of variables of this type does not change whether a form has rational zeros, we may assume in the proof of Theorem 1.1 that F has the properties listed in this lemma.

Our final Lemma in this section is due to Bovey [15].

Lemma 3.5. *Let $n \in \mathbb{Z}^+$, and suppose that for $i = 0, \dots, n$, we have $F_i = \sum_{j=1}^{m_i} a_{ij} x_{ij}$ with all the a_{ij} odd and with $\sum_{i=0}^{k-1} m_i \geq 2^k$ for each $k = 1, \dots, n$. Then for any positive integer $N > n$, the form $\sum_{i=0}^{n} 2^i F_i$ represents at least $\min\{\sum_{i=0}^{n} m_i, 2^N\}$ different residue classes modulo 2^N, where the $x_{ij} \in \{0, 1\}$ and $x_{0j} = 1$ for at least one j.*

4. Proof of the Theorem - The Easy Cases

In this section, we prove Theorem 1.1 in the case where d is odd (so that $\gamma = 1$) and the case where d is even and $\gamma | d$. Note that the definition of γ is such that we never have $\gamma = 2$.

Lemma 4.1. *Suppose that d is odd. Then we have $\Gamma_2^*(d) = d + 1$, as in Theorem 1.1.*

Proof. This lemma is a special case of [19, Lemma 10], and so we will only briefly sketch the proof. With $d + 1$ variables distributed between levels $0, \dots, d - 1$, there must be some level which contains two variables. These variables can be contracted to a higher level, which (since $\gamma = 1$) immediately leads to a 2-adic solution by Lemma 2.1. This shows that $\Gamma_2^*(d) \leq d + 1$. By the remarks following the statement of Theorem 1.1, we know that $\Gamma_2^*(d) \geq d + 1$, which completes the proof of the lemma.

□

Lemma 4.2. *Suppose that $d \neq 2$ is even and write $d = 2^\tau d_0$, where d_0 is odd. Then $\gamma = \tau + 2$. Suppose that $\gamma | d$, with $d = \gamma q$. Then we have $\Gamma_2^*(d) = (2^\gamma - 1)q + 1$, as in Theorem 1.1.*

Proof. As above, we only need to show that this is an upper bound for $\Gamma_2^*(d)$. Hence we assume that there are exactly $(2^\gamma - 1)q + 1$ variables in F. Write F in the form given in Lemma 3.4. We will show that it is always possible to find a solution of the congruence

$$F \equiv 0 \pmod{2^\gamma} \tag{4}$$

with at least one odd variable at level 0. As in Lemma 3.4, let m_i be the number of variables at level i. Then by Lemma 3.5 (with $n = \tau + 1$ and $N = \gamma = \tau + 2$), we can find our desired solution if we can show that $m_0 + \dots + m_{k-1} \geq 2^k$ for $1 \leq k \leq \gamma$. (We note as a subtle point that since $\tau + 1 \leq d - 1$, it is legitimate for us to consider variables at levels up to

$\tau+1$.) In order to prove these inequalities, by Lemma 3.4 it is sufficient to show that

$$\frac{k\left((2^{\gamma}-1)q+1\right)}{\gamma q} > 2^k - 1 \tag{5}$$

for $1 \leq k \leq \gamma$. Further, we note that if we can prove that the $k=1$ and $k=\gamma$ cases of (5) hold, then Lemma 3.1 shows that the other cases of (5) also hold.

The $k=1$ case of (5) simply states that

$$\frac{(2^{\gamma}-1)q+1}{\gamma q} > 1,$$

and this is easily seen to be true since $2^{\gamma}-1 > \gamma$ for any integer $\gamma \geq 2$. It is also trivial to see that the $k=\gamma$ case holds, since then the left-hand side of the inequality (5) reduces to $2^{\gamma}-1+\frac{1}{q}$. As stated above, Lemmas 3.1 and 3.5 now show that we can find a solution of $F \equiv 0 \pmod{2^{\gamma}}$ with at least one odd variable at level 0. This solution now lifts to a nontrivial 2-adic solution by Lemma 2.1.

□

5. Completion of the Proof

In this section, we complete the proof of Theorem 1.1. As above, it suffices to show that the formula in the theorem is an upper bound for $\Gamma_2^*(d)$. After the results of Section 4, we may assume that $d \neq 2$ is even (so that $\gamma \geq 3$) and that $r > 0$. For convenience, in this section we will write everything in terms of τ rather than γ, keeping in mind that $\gamma = \tau+2$. Let $s = (2^{\tau+2}-1)q + 2^r$. By Lemma 3.4, we may assume that we have $m_0 + \cdots + m_{k-1} \geq ks/d$ for $1 \leq k \leq d$.

From this, Lemma 3.2 and the fact that the m_i are integers show that $m_0 + \cdots + m_{k-1} \geq 2^k$ for $1 \leq k \leq \tau+1$. If we additionally have $m_0 + \cdots + m_{\tau+1} \geq 2^{\tau+2}$, then by Lemma 3.5 we can represent the zero residue modulo $2^{\tau+2}$ with at least one variable from F_0 not equal to zero. Then Hensel's Lemma guarantees a nontrivial p-adic zero of F, and we are done. Hence we may assume that $m_0 + \cdots + m_{\tau+1} \leq 2^{\tau+2} - 1$.

Suppose that for some number t with $1 \leq t \leq q-1$, we can find t pairwise disjoint sets of subscripts $S_1, \ldots, S_t$ with the following properties:

1. $S_i \subseteq \{0, 1, 2, \dots, d-1\}$ for each i,
2. $|S_i| = \tau + 2$ for each i,
3. the elements of each S_i are consecutive integers $s_i, s_i + 1, \dots, s_i + \tau + 1$,
4. for each i and each k with $1 \le k \le \tau + 1$, we have $m_{s_i} + \cdots + m_{s_i+k-1} \ge 2^k$,
5. for each i, we have $m_{s_i} + \cdots + m_{s_i+\tau+1} \le 2^{\tau+2} - 1$.

By the previous paragraph, we may take $S_1 = \{0, 1, \dots, \tau + 1\}$, and so at least one such set exists. We now show that either we can find a nontrivial solution of $F = 0$ or else an additional set exists with the above properties.

Consider the forms F_j (as defined in the statement of Lemma 3.4) where $j \notin \cup S_i$. There are $\alpha = (\tau + 2)(q - t) + r$ such forms, and they contain a total of at least $(2^{\tau+2} - 1)(q - t) + 2^r$ variables. Suppose that these forms are $F_{i_0}, \dots, F_{i_\alpha}$, with $0 \le i_0 < i_1 < \cdots < i_\alpha \le d - 1$. By Lemma 3.3, we may relabel these forms as $F_{w_0}, \dots, F_{w_\alpha}$ in such a way that

1. the ordered tuple $(w_0, w_1, \dots, w_\alpha)$ is a cyclic permutation of the tuple $(i_0, i_1, \dots, i_\alpha)$, and
2. for each k with $1 \le k \le \alpha$, we have

$$m_{w_0} + \cdots + m_{w_{k-1}} \ge \frac{k\left(\left(2^{\tau+2} - 1\right)(q - t) + 2^r\right)}{(\tau + 2)(q - t) + r}.$$

By Lemma 3.2 and the fact that the m_i are all integers, we have

$$m_{w_0} + \cdots + m_{w_{k-1}} \ge 2^k \qquad \text{for} \qquad 1 \le k \le \tau + 1.$$

Now, suppose that the subscripts $w_0, \dots, w_{\tau+1}$ are *not* consecutive numbers. Then there is a smallest number $k \le \tau$ such that $w_k = w_0 + k$, but $w_{k+1} \ne w_0 + k + 1$. Then $w_k + 1$ is the smallest element of one of the sets S_i defined above. (If we have $w_k = d - 1$, we may temporarily apply the change of variables $x' = x/p$ to all variables at levels $0, 1, \dots, \tau + 1$, bringing them to levels $d, d + 1, \dots, d + \tau + 1$. Then we may temporarily consider $s_1 = d$ and $S_1 = \{d, \dots, d + \tau + 1\}$.) That is, we have $w_k + 1 = s_i$ for some i. By Lemma 3.5, we can solve the congruence

$$2^{w_0} F_{w_0} + \cdots + 2^{w_k} F_{w_k} \equiv 0 \pmod{2^{w_k+1}}$$

with at least one variable from F_{w_0} nonzero. If our solution to this congruence is actually a solution modulo $2^{w_0+\tau+2}$, then this lifts to a 2-adic solution by Hensel's Lemma. If not, then we can contract the variables used in this solution to a variable y, with coefficient a_y, at some level 2^{w_0+k+l}, where $k+1 \leq k+l \leq \tau+1$. Now consider the form $2^{s_i}F_{s_i} + \cdots + 2^{s_i+\tau}F_{s_i+\tau}$. By Lemma 3.5, this form represents every multiple of 2^{s_i} modulo $2^{s_i+\tau+1}$. If we set $y = 1$, then since a_y is divisible by 2^{s_i} we can solve the congruence $a_y + 2^{s_i}F_{s_i} + \cdots + 2^{s_i+\tau}F_{s_i+\tau} \equiv 0 \pmod{2^{s_i+\tau+1}}$. This yields a solution of the congruence $F \equiv 0 \pmod{2^{s_i+\tau+1}}$ which involves a nonzero variable at level w_0. Since $s_i + \tau + 1 \geq w_0 + \tau + 2$, this lifts to a 2-adic solution by Hensel's Lemma. We therefore see that if the numbers $w_0, \ldots, w_{\tau+1}$ are not consecutive, then the equation $F = 0$ has a nontrivial 2-adic solution.

Hence we may assume that the numbers $w_0, \ldots, w_{\tau+1}$ are consecutive. Set $S_{t+1} = \{w_0, \ldots, w_{\tau+1}\}$. We have already shown that this set satisfies properties 1-4 above. If we have $m_{w_0} + \cdots + m_{w_{\tau+1}} \geq 2^{\tau+2}$, then Lemma 3.5 shows that we can solve the congruence

$$2^{w_0}F_{w_0} + \cdots + 2^{w_{\tau+1}}F_{w_{\tau+1}} \equiv 0 \pmod{2^{w_0+\tau+2}}$$

with at least one variable from F_{w_0} not equal to zero, and this lifts to a 2-adic solution by Hensel's Lemma. Therefore we may assume that $m_{w_0} + \cdots + m_{w_{\tau+1}} \leq 2^{\tau+2} - 1$, which is the final desired property.

Continuing, we may assume that we can find a total of q mutually disjoint sets $S_1, \ldots, S_q$ of subscripts having the five listed properties, since otherwise the equation $F = 0$ would have a solution and we would be done. Hence there are exactly r subscripts j such that $j \notin \cup S_i$. The forms F_j contain a total of at least 2^r variables. Suppose that these forms are $F_{i_0}, \ldots, F_{i_{r-1}}$, with $0 \leq i_0 < i_1 < \cdots < i_{r-1} \leq d-1$. By Lemma 3.3, we may relabel these forms as $F_{w_0}, \ldots, F_{w_{r-1}}$ in such a way that

1. the ordered r-tuple $(w_0, w_1, \ldots, w_{r-1})$ is a cyclic permutation of the r-tuple $(i_0, \ldots, i_{r-1})$, and
2. for each k with $1 \leq k \leq r$, we have

$$m_{w_0} + \cdots + m_{w_{k-1}} \geq \frac{k \cdot 2^r}{r}.$$

(Note that this changes the meaning of the numbers i_j and w_j from above.) We now proceed as before. It is easy to see that we have $m_{w_0} \geq 2$ and

$m_{w_0} + \cdots + m_{w_{r-1}} \geq 2^r$. Thus Lemma 3.1 implies that

$$m_{w_0} + \cdots + m_{w_{k-1}} \geq 2^k \qquad \text{for} \qquad 1 \leq k \leq r.$$

Let k be the smallest number such that $w_k = w_0 + k$, but $w_{k+1} \neq w_0 + k + 1$. Then $w_k + 1$ is the smallest element of one of the sets S_i, and we have $w_k + 1 = s_i$ for some i. (Again, if $w_k = d - 1$, then by a change of variables we may consider S_1 to be the set $\{d, \ldots, d + \tau + 1\}$ and $s_1 = d$.) By Lemma 3.5, we can solve the congruence

$$2^{w_0} F_{w_0} + \cdots + 2^{w_k} F_{w_k} \equiv 0 \pmod{2^{w_k+1}}$$

with at least one variable from F_{w_0} nonzero. If our solution to this congruence is actually a solution modulo $2^{w_0+\tau+2}$, then it lifts to a 2-adic solution by Hensel's Lemma. If not, then we can contract the variables used in this solution to a variable y at some level 2^{w_0+k+l}, where $k+1 \leq k+l \leq \tau+1$. Let a_y be the coefficient of this variable. Now consider the form $2^{s_i} F_{s_i} + \cdots + 2^{s_i+\tau} F_{s_i+\tau}$. By Lemma 3.5, this form represents every multiple of 2^{s_i} modulo $2^{s_i+\tau+1}$. If we set $y = 1$, then we can solve the congruence $a_y + 2^{s_i} F_{s_i} + \cdots + 2^{s_i+\tau} F_{s_i+\tau} \equiv 0 \pmod{2^{s_i+\tau+1}}$. As before, this leads to a solution of $F \equiv 0 \pmod{2^{s_i+\tau+1}}$ which involves a nonzero variable at level w_0, and this solution lifts to a 2-adic solution by Hensel's Lemma. This completes the proof of Theorem 1.1.

6. Acknowledgements

The author would like to thank David Leep for pointing out an error in an early draft of this article. Parts of this work were completed while the author was enjoying the generous hospitality of the Universidade de Brasília while on sabbatical leave.

Appendix A. Bibliography

[1] R. Brauer, "A note on systems of homogeneous algebraic equations", Bull. Amer. Math. Soc. 51 (1945) 749–755.

[2] H. Davenport, D. J. Lewis, "Homogeneous additive equations", Proc. Royal Soc. London Ser. A 274 (1963) 443–460.

[3] J. Brüdern, H. Godinho, “On Artin’s conjecture, I: systems of diagonal forms”, Bull. London Math. Soc. 31 (1999) 305–313.

[4] J. Brüdern, H. Godinho, “On Artin’s conjecture, II: pairs of additive forms”, Proc. London Math. Soc. 84 (2002) 513–538.

[5] H. Davenport, D. J. Lewis, “Two additive equations”, Proc. Symposia Pure Math. (Houston) 12 (1967) 74–98.

[6] H. Davenport, D. J. Lewis, “Simultaneous equations of additive type”, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. 264 (1969) 557–595.

[7] M. Dodson, “homogeneous additive congruences”, Philos. Trans. Roy. Soc. London Ser. A 261 (1967) 163–210.

[8] M. Dodson, “Some estimates for diagonal equations over $\mathfrak{p}$-adic fields”, Acta Arith. 40 (1982) 117–124.

[9] M. Knapp, “Systems of diagonal equations over p-adic fields”, J. London Math. Soc. (2) 63 (2001) 257–267.

[10] M. Knapp, “Diagonal equations of different degrees over p-adic fields”, Acta Arith. 126.2 (2007) 139–154.

[11] L. Low, J. Pitman, A. Wolff, “Simultaneous diagonal congruences”, J. Number Theory 29 (1988) 31–59.

[12] T. D. Wooley, “Artin’s conjecture and systems of diagonal equations”, Forum Math. (to appear).

[13] R. G. Bierstedt, Some problems on the distribution of kth power residues modulo a prime, Ph.D. thesis, University of Colorado (1963).

[14] K. K. Norton, On homogeneous diagonal congruences of odd degree, Ph.D. thesis, University of Illinois (1966).

[15] J. D. Bovey, “$\Gamma^*(8)$”, Acta Arith. 25 (1974) 145–150.

[16] M. Knapp, “Exact values of the function $\Gamma^*(k)$”, J. Number Theory 131 (2011) 1901–1911.

[17] D. S. Veras, Formas aditivas sobre corpos p-ádicos, Ph.D. thesis, Universidade de Brasília (2017).

[18] M. Knapp, “Pebbling on directed cycle graphs”, (in preparation).

[19] M. Knapp, “Pairs of additive forms of odd degrees”, Michigan Math J. 61 (2012) 493–505.