Test Ideals in Diagonal Hypersurface Rings

Moira A. McDermott

Department of Mathematics and Computer Science, Gustavus Adolphus College,
800 West College Avenue, St. Peter, Minnesota 56082-1498
E-mail: mmcdermo@gac.edu

Let \( R = k[x_1, \ldots, x_n]/(x_1^d + \cdots + x_n^d) \), where \( k \) is a field of characteristic \( p \), \( p \) does not divide \( d \), and \( n \geq 3 \). If \( p < d \), then the test ideal for \( R \) is contained in \((x_1, \ldots, x_n)^{p-1}\). If \( d = p+1 \), then the test ideal for \( R \) is equal to \((x_1, \ldots, x_n)^{p-1}\).

Key Words: test ideal, tight closure, characteristic \( p \)

INTRODUCTION

In this paper we determine the test ideal for diagonal hypersurface rings where the characteristic is one less than the degree of the defining equation. Test elements and test ideals were introduced by Hochster and Huneke in [4]. They have been studied further in [5], [6], [1] and [12], for example. The existence of test elements is an important theorem in the theory of tight closure and the theory of test elements has an important application in proving that tight closure persists under certain base changes [5, (6.24)]. Given the difficulty in computing tight closure, even for a fixed ideal, using specified test elements is often the only practical way to compute tight closure.

Huneke and Smith formulate a tight closure interpretation of the Kodaira Vanishing Theorem [10]. One form of the Vanishing Conjecture for Gorenstein Rings [10, (5.4)] asserts that if \((S, m)\) is an \(\mathbb{N}\)-graded Noetherian Gorenstein domain over a field \( S_0 \) of characteristic zero or \( p \gg 0 \), then the test ideal for \( S \) is exactly the ideal generated by elements of degree greater than \( a \), where \( a \) is the \( a \)-invariant of \( S \). They prove that the Vanishing Conjecture is true in dimension two provided that \( S \) is an equidimensional two-dimensional graded ring over a perfect field \( k = S_0 \) with an isolated singularity and the characteristic is zero or exceeds the degrees of a minimal set of generators for the modules of \( k \)-linear derivations of the normalizations [10, (4.5)]. They also point out that the conjecture is true for hypersurface rings with a similar restriction on the characteristic. See [9, (6.4)] for a direct proof of the Strong Vanishing Theorem for Hypersurfaces. Hara’s
recent work on rational singularities and F-rational singularities gives a proof of the Vanishing Conjecture for finitely generated \( k \)-algebras where \( k \) is a field of characteristic zero [3]. For \( k[x_1, \ldots, x_n]/(x_1^d + \cdots + x_n^d) \), where \( k \) is a field of characteristic \( p \), if \( d > n \), then the test ideal is \((x_1, \ldots, x_n)^{d-n+1}\) for sufficiently large \( p \). If \( d < n \), then the ring is F-regular [2, (2.11)] and the test ideal is the unit ideal, again for sufficiently large \( p \). If \( n = d \), then the Strong Vanishing Theorem holds when \( p > d \). Thus for rings of the form \( k[x_1, \ldots, x_d]/(x_1^d + \cdots + x_d^d) \), where \( k \) is a field of characteristic \( p \) and \( p > d \), the test ideal is the maximal ideal.

We are interested in determining the test ideal in diagonal hypersurface rings when \( p < d \). When \( p = d \), the ring is not a domain and is not of great interest. If \( R = k[x_1, \ldots, x_d]/(x_1^d + \cdots + x_d^d) \) with \( p < d \), then the test ideal is contained in \((x_1, \ldots, x_d)^{p-1}\) which is smaller than expected in many cases. When \( d = p + 1 \) we show that the test ideal is \((x_1, \ldots, x_d)^{p-1}\).

1. TIGHT CLOSURE

We review the definition of tight closure for ideals of rings of characteristic \( p > 0 \). Tight closure is defined more generally for modules and also for rings containing fields of arbitrary characteristic. See [4] or [8] for more details.

**Definition 1.1.** Let \( R \) be a ring of characteristic \( p \) and \( I \) be an ideal in a Noetherian ring \( R \) of characteristic \( p > 0 \). An element \( x \in R \) is in the **tight closure** of \( I \), denoted \( I^* \), if there exists an element \( c \in R \), not in any minimal prime of \( R \), such that for all \( q = pf \), \( cx^q \in I^{[q]} \) where \( I^{[q]} \) is the ideal generated by the \( q \)th powers of all elements of \( I \).

In many applications one would like to be able to choose the element \( c \) in the definition of tight closure independent of \( x \) or \( I \). It is very useful when a single choice of \( c \), a test element, can be used for all tight closure tests in a given ring.

**Definition 1.2.** The ideal of all \( c \in R \) such that for any ideal \( I \subseteq R \), we have \( cu^q \in I^{[q]} \) for all \( q \) whenever \( u \in I^* \) is called the **test ideal** for \( R \). An element of the test ideal that is not in any minimal prime is called a **test element**.

2. \( \mathbb{Z}_n \)-GRADING

We will make use of the following grading in our calculation of the test ideal. We denote by \( \mathbb{Z}_n \) the ring \( \mathbb{Z}/n\mathbb{Z} \). Next we describe a \( \mathbb{Z}_n \)-grading of rings of the form \( R = A[z]/(z^n - a) \) where \( a \in A \). The ring \( R \) has the following decomposition as an \( A \)-module:

\[
R = A \oplus A z \oplus \cdots \oplus A z^{n-1}.
\]
This is true because every element of \( R \) can be uniquely expressed as an element of 
\( A \oplus A z_1 \oplus \cdots \oplus A z^{n-1} \) by replacing every occurrence of \( z^n \) by \( a \). \( R \) is \( \mathbb{Z}_{n} \)-graded, 
where the \( i \)th piece of \( R \), denoted by \( R_i \), is \( A z^i \), \( 0 \leq i < n \), since \( A z^i A z^j \subseteq A z^{i+j} \) 
if \( i + j < n \) and \( A z^i A z^j \subseteq A z^{i+j-n} \) if \( i + j \geq n \).

We use this idea to obtain multiple \( \mathbb{Z}_{n} \)-gradings of \( R = k[x_1, \ldots, x_n]/(x_1^d + \cdots + x_n^d) \), where \( k \) is a field of characteristic \( p \). Let \( z = x_i \) and \( A = k[x_1, \ldots, x_i, \ldots, x_n] \).

We now show that if \( I \) is a graded ideal, then so is \( I^* \).

**Lemma 2.1.** Let \( R \) be a finitely generated \( k \)-algebra that is \( \mathbb{Z}_{n} \)-graded and of 
characteristic \( p \), where \( p \) is not a prime factor of \( n \) (\( p = 0 \) is allowed). Then the 
tight closure of a homogeneous ideal of \( R \) is homogeneous.

**Proof.** Without loss of generality, we can assume \( R \) is reduced, since the tight 
closure of \( I \) is the preimage of the tight closure of the image of \( I \) modulo the 
nilradical. Because the singular locus of \( R \) is defined by a homogeneous ideal not 
contained in any minimal prime, \( R \) has a homogeneous test element, say \( c \). Let \( I \) be 
a homogeneous ideal, and suppose that \( z = z_0 + z_1 + \cdots + z_{n-1} \) is in \( I^* \), where \( z_i \) 
is the homogeneous component of \( z \) of degree \( i \) mod \( n \). Now we have \( cz^q = cz_0^q + 
z_i^q + \cdots + cz_{n-1}^q \) is in the homogeneous ideal \( I^q \), and hence each of its 
homogeneous components is in \( I^q \). But each of the elements \( cz_i^q \) is homogeneous of degree 
\( qi + \deg c \mod n \), and since \( q \) is invertible in \( \mathbb{Z}_n \), these all have distinct degrees. Thus 
each \( cz_i^q \in I^q \) for all \( q \gg 0 \) and each \( z_i \in I^* \). This shows that \( I^* \) is homogeneous.

**3. THE TEST IDEAL**

**Theorem 3.1.** Let \( R = k[x_1, \ldots, x_n]/(x_1^d + \cdots + x_n^d) \) where \( k \) is a field of 
characteristic \( p \), \( p \) does not divide \( d \), and \( n \geq 3 \). Let \( \tau \) be the test ideal for \( R \). If 
\( p < d \), then \( \tau \subseteq (x_1, \ldots, x_n)^{p-1} \).

**Proof.** We know that in a Gorenstein local ring with \( m \)-primary test ideal, the 
test ideal is \((t_1, \ldots, t_n) : (t_1, \ldots, t_n)^{\ast} \) where \( t_1, \ldots, t_n \) is a system of parameters 
consisting of test elements [8, Ex. 2.14],[9]. We also know that the elements of 
the Jacobian ideal are always test elements [7, (1.5.5)]. This is actually a rather 
deep result in that it uses the main results of the Lipman-Sathaye theorem [11]. In 
this case we have that \( x_1^{d-1}, \ldots, x_n^{d-1} \) are test elements. We will not use the full 
force of this result yet. Instead we will just use the fact that \( x_1^d, \ldots, x_n^d \) are test 
elements. Thus it is sufficient to show that

\[
(x_1^d, \ldots, x_n^d)^{\ast} : R(x_1^d, \ldots, x_n^d)^{\ast} \subseteq (x_1, \ldots, x_n)^{p-1}.
\]
This is equivalent to showing that

\[(x_1^d, \ldots, x_{n-1}^d) : R(x_1, \ldots, x_n)^p \subseteq (x_1^d, \ldots, x_{n-1}^d)^* \]

To see this, let \( I = (x_1^d, \ldots, x_{n-1}^d) \) and note that \( R/I \) is a zero-dimensional Gorenstein ring, and so is also the injective hull of the residue field. The equivalence follows from duality.

Let \( R = k[x_1, \ldots, x_n]/(x_1^d + \cdots + x_{n-1}^d) \) and \( S = k[x_1, \ldots, x_n] \). It follows from a direct computation that

\[(x_1^d, \ldots, x_{n-1}^d) : R(x_1, \ldots, x_n)^p \subseteq (x_1^d, \ldots, x_{n-1}^d, x_n^p) : S(x_1, \ldots, x_n)^p R \).

Hence it is sufficient to show that

\[(x_1^d, \ldots, x_{n-1}^d, x_n^p) : S(x_1, \ldots, x_n)^p R \subseteq (x_1^d, \ldots, x_{n-1}^d)^* \]

Our next claim is that the test ideal for \( R \) can be generated by monomials. Recall that there is a \( \mathbb{Z}_n \)-grading of \( R \) associated with each \( x_i \), \( 1 \leq i \leq n \). We also know that if \( I \) is a homogeneous ideal, then so are \( I^* \) (2.1) and \( I : I^* \).

Since \((x_1^d, \ldots, x_{n-1}^d) \) is homogeneous with respect to each of the gradings, so is \((x_1^d, \ldots, x_{n-1}^d, x_n^p) : R(x_1^d, \ldots, x_{n-1}^d)^* \) and hence so is the test ideal. Using the grading with respect to each \( x_i \), the multigrading, we see that the test ideal can be generated by monomials. Essentially, this is because only monomials are homogeneous with respect to all \( n \) gradings simultaneously.

It is routine to check using standard manipulations of monomial ideals that

\[(x_1^d, \ldots, x_n^d) : S(x_1, \ldots, x_n)^p = (x_1^d, \ldots, x_{n-1}^d) + (x_1, \ldots, x_n)^{(n-1)(d-1)+d-p+1} \cdot (x_1^d, \ldots, x_n^d) \]

Suppose \( u \in (x_1, \ldots, x_n)^{(n-1)(d-1)+d-p+1} \) is a monomial and \( w \in (x_1, \ldots, x_n)^p \).

The degree of \( uw \) is at least \( n(d-1) + 1 \) and it follows from a counting argument that \( uw \in (x_1, \ldots, x_n)^{(n-1)(d-1)+d-p+1} \cdot (x_1^d, \ldots, x_n^d) \). Hence any element of \((x_1, \ldots, x_n)^{(n-1)(d-1)+d-p+1} \cdot (x_1^d, \ldots, x_n^d) \) is in \((x_1^d, \ldots, x_n^d) : S(x_1, \ldots, x_n)^p \). Now let \( u = x_1^{a_1} \cdots x_n^{a_n} \), and suppose \( \sum_{i=1}^n a_i \leq (n-1)(d-1)+d-p \) and \( u \in (x_1^d, \ldots, x_n^d) : S(x_1, \ldots, x_n)^p \).

Let \( z = x_1^{d-1-a_1} \cdots x_n^{d-1-a_n} \). Observe that \( z \in (x_1, \ldots, x_n)^p \) since \( z \) has the correct degree. By assumption then \( uz \in (x_1^d, \ldots, x_n^d) \). But

\[uz = x_1^{d-1} \cdots x_n^{d-1} \notin (x_1^d, \ldots, x_n^d) \]

Let \( I = (x_1^d, \ldots, x_n^d) \). Note that \((x_1^d, \ldots, x_n^d) : R = IR \). Next we show that \( I + m^{(n-1)(d-1)+d-p+1} \subseteq I^* \). Let \( u = x_1^{a_1} \cdots x_n^{a_n} \in m^{(n-1)(d-1)+d-p+1} \). Note that if \( su \) \( \in I^w \), then \( u \in I^w \) since \( u \in I^w \). Thus it is sufficient to show that

\[(x_1^{a_1} \cdots x_n^{a_n})^p \in I^{[p]} = (x_1^d, \ldots, x_n^d) \]
Using the basic relation in $R$ we can write
\[ -x_n^{a_n-p} = (-x_n^d)^{a_n-d+p}(-x_n^{d-a_n})(d-p) \]
\[ = (x_1^d + \cdots + x_{n-1}^d)^{a_n-d+p}(-x_n^{d-a_n})(d-p). \]

Hence it is sufficient to see that
\[ x_1^{a_1d} \cdots x_{n-1}^{a_{n-1}d}(x_1^d + \cdots + x_{n-1}^d)^{a_n-d+p} \in (x_1^{dp}, \ldots, x_{n-1}^{dp}). \]

This will be true if for all $i_1, \ldots, i_{n-1} \geq 0$ such that $i_1 + \cdots + i_{n-1} = a_n - d + p$ we have
\[ a_\nu p + i_\nu d \geq dp \quad \text{for some } \nu \text{ with } 1 \leq \nu \leq n - 1. \]

Suppose, on the contrary, that there exist $i_1, \ldots, i_{n-1} \geq 0$ with $i_1 + \cdots + i_{n-1} = a_n - d + p$ and such that $a_\nu p + i_\nu (p+1) \leq dp - 1, 1 \leq \nu \leq n - 1$. Then because each $i_\nu$ is a non-negative integer, we have
\[ i_\nu \leq \left\lfloor \frac{dp - 1 - a_\nu p}{d} \right\rfloor \leq \left\lfloor \frac{p(d-a_\nu) - 1}{d} \right\rfloor \leq d - a_\nu - 1. \]

So the sum
\[ a_n - d + p = \sum_{\nu=1}^{n-1} i_\nu \leq \sum_{\nu=1}^{n-1} d - a_\nu - 1 \]
\[ \leq (n-1)(d-1) - \sum_{\nu=1}^{n-1} a_\nu \]
\[ \leq (n-1)(d-1) - ((n-1)(d-1) + d - p + 1 - a_n) \]
\[ \leq a_n - d + p - 1, \]

and this is a contradiction.

**Theorem 3.2.** Let $R = k[x_1, \ldots, x_n]/(x_1^{p+1} + \cdots + x_n^{p+1})$ where $k$ is a field of characteristic $p$ and $n \geq 3$. Then $(x_1, \ldots, x_n)^{p-1}$ is the test ideal for $R$.

**Proof.** We know from 3.1 that the test ideal is contained in $(x_1, \ldots, x_n)^{p-1}$. It remains to show the other inclusion. Recall that the test ideal can be computed as $(t_1, \ldots, t_n) : (t_1, \ldots, t_n)^*$ where $t_1, \ldots, t_n$ is a system of parameters
consisting of test elements and that the elements of the Jacobian ideal are always test elements. Thus \(x_1^p, \ldots, x_{n-1}^p\) are test elements, and the test ideal is 
\((x_1^p, \ldots, x_{n-1}^p) : R(x_1^p, \ldots, x_{n-1}^p)^*\). Hence it is sufficient to show that 
\[(x_1, \ldots, x_n)^{p-1} \subseteq (x_1^p, \ldots, x_{n-1}^p) : R(x_1^p, \ldots, x_{n-1}^p)^*\.
As before, this is equivalent to showing that 
\[(x_1^p, \ldots, x_{n-1}^p)^* \subseteq (x_1^p, \ldots, x_{n-1}^p) : R(x_1^p, \ldots, x_{n-1}^p)^{p-1}\]
by duality.

Let \(R = k[x_1, \ldots, x_n]/(x_1^{p+1} + \cdots + x_n^{p+1})\) and \(S = k[x_1, \ldots, x_n]\). It follows from a direct computation that 
\[(x_1^p, \ldots, x_{n-1}^p) : R(x_1^p, \ldots, x_{n-1}^p)^{p-1} = (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) : s(x_1, \ldots, x_n)^{p-1})R.

Hence it is sufficient to show that 
\[(x_1^p, \ldots, x_{n-1}^p)^* \subseteq ((x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) : s(x_1, \ldots, x_n)^{p-1})R.
It is routine to check using standard manipulations of monomial ideals that 
\[(x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) : s(x_1, \ldots, x_n)^{p-1}
= (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) + (x_1, \ldots, x_n)^{(n-1)(p-1)+2}.
Suppose \(u \in (x_1, \ldots, x_n)^{(n-1)(p-1)+2}\) is a monomial and \(w \in m^{p-1}\). The degree of \(uw\) is at least \(n(p-1)+2\) and it follows by a counting argument that \(uw \in (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1})\). Hence any element of \((x_1, \ldots, x_n)^{(n-1)(p-1)+2}\) is in 
\((x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) : s(x_1, \ldots, x_n)^{p-1}\). Now let \(u = x_1^{a_1} \cdots x_n^{a_n}\), and suppose 
\[\sum_{i=1}^{n} a_i \leq (n-1)(p-1)+1\] and \(u \in (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) : s(x_1, \ldots, x_n)^{p-1}.
Let \(z = x_1^{p-1-a_1} \cdots x_{n-1}^{p-1-a_{n-1}} x_n^{p-a_n}\). Observe that \(z \in (x_1, \ldots, x_n)^{p-1}\) since 
z has the correct degree. By assumption then \(uz \in (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1})\). But 
\[uz = x_1^{p-1} \cdots x_{n-1}^{p-1} x_n^p \notin (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}).
It remains to show that 
\[(x_1^p, \ldots, x_{n-1}^p)^* \subseteq (x_1^p, \ldots, x_{n-1}^p, x_n^{p+1}) + (x_1, \ldots, x_n)^{(n-1)(p-1)+2}.
Suppose \(a_1 < p, \ldots, a_{n-1} < p, a_n < p+1\) and \(\sum_{i=1}^{n} a_i \leq (n-1)(p-1)+1\). We claim that 
\(x_1^{a_1} \cdots x_n^{a_n} \notin (x_1^p, \ldots, x_{n-1}^p)^*\). Since \(x_1^p, \ldots, x_{n-1}^p\) are test elements, it is sufficient to show that 
\[(x_1^p, \ldots, x_{n-1}^p)(x_1^{a_1} \cdots x_n^{a_n})^{p^2} \notin (x_1^p, \ldots, x_{n-1}^p)^{[p^2]} = (x_1^{p^2}, \ldots, x_{n-1}^{p^2}).\]
This is equivalent to showing \((x_1^{a_1} \cdots x_n^{a_n})^{p^2} \not\in (x_1^{p^2}, \ldots, x_n^{p^2}) : (x_1^p, \ldots, x_n^p)\) or

\[(x_1^{a_1} \cdots x_n^{a_n})^{p^2} \not\in (x_1^{p^2}, \ldots, x_{n-1}^{p^2}, (x_1 \cdots x_{n-1})^{p^2-p}).\]

Using the fact that \(a_n p^2 = a_n (p^2 - 1) + a_n\) and the basic relation in \(R\) we can write

\[(x_1^{a_1} \cdots x_n^{a_n})^{p^2} = \pm x_1^{a_1 p^2} \cdots x_{n-1}^{a_{n-1} p^2} (x_1^{p+1} + \cdots + x_{n-1}^{p+1})^{\alpha_n (p-1)} x_n^{a_n}.

So it is now sufficient to show that

\[x_1^{a_1 p^2} \cdots x_{n-1}^{a_{n-1} p^2} (x_1^{p+1} + \cdots + x_{n-1}^{p+1})^{\alpha_n (p-1)} x_n^{a_n} \not\in (x_1^{p^2}, \ldots, x_{n-1}^{p^2}, (x_1 \cdots x_{n-1})^{p^2-p}).\]

If we expand using the binomial theorem, then we want \(b_1, \ldots, b_{n-1}\) such that

\[
\begin{align*}
b_1 + \cdots + b_{n-1} &= a_n (p - 1) \quad (1) \\
p^2 a_j + b_j (p + 1) &< p^3 \quad \text{all } j \\
p^2 a_j + b_j (p + 1) &< p^3 - p \quad \text{some } j
\end{align*}
\]

and

\[
\begin{pmatrix} a_n (p - 1) \\ b_1, \ldots, b_{n-1} \end{pmatrix} \not\equiv 0 \mod p. \quad (4)
\]

Since

\[
\begin{pmatrix} a_n (p - 1) \\ b_1, \ldots, b_{n-1} \end{pmatrix} = \frac{(a_n (p - 1))!}{b_1! \cdots b_{n-1}!},
\]

condition (4) will be satisfied as long as there are the same number of factors of \(p\) occurring in the numerator as in the denominator of the right-hand side of the previous equation. By (1),

\[
b_i \leq a_n (p - 1) < (p + 1)(p - 1) = p^2 - 1.
\]

In this case \([b_i/p]\) equals the number of factors of \(p\) in \(b_i!\) where \([n]\) denotes the integer part of \(n\). So condition (4) will be satisfied if

\[
\begin{align*}
\left[ \frac{b_1}{p} \right] + \cdots + \left[ \frac{b_{n-1}}{p} \right] &= \left[ \frac{a_n (p - 1)}{p} \right] \\
&= \left[ a_n - \frac{a_n}{p} \right] \\
&= a_n - 1.
\end{align*}
\]
Condition (2) implies that

\[
p^2a_j + b_j(p + 1) \leq p^3 - 1
\]
\[
b_j(p + 1) \leq p^3 + 1 - p^2a_j + a_j - a_j - 2
\]
\[
b_j \leq p^2 - p + 1 - a_j(p - 1) - \frac{a_j + 2}{p + 1}
\]
\[
b_j \leq p^2 - p - a_j(p - 1),
\]
while condition (3) implies that

\[
b_j(p + 1) < p^3 - p - p^2a_j
\]
\[
b_j < p^2 - p - a_j(p - 1) - \frac{a_j}{p + 1}
\]
\[
b_j \leq p^2 - p - a_j(p - 1) - 1.
\]

So we need all of the \(b_j \leq p^2 - p - a_j(p - 1)\) and one of them one less. If we choose the \(b_j\)'s maximal with respect to satisfying condition (2) and ignore condition (3) for now, then \(b_1 + \cdots + b_{n-1} = (n - 1)(p^2 - p) - \sum_{j=1}^{n-1} a_j(p - 1)\), but we need \(b_1 + \cdots + b_{n-1} = a_n(p-1)\). We are assuming that \(a_1 + \cdots + a_n = (n-1)(p-1)+1\), so the difference is

\[
b_1 + \cdots + b_{n-1} - a_n(p - 1) = ((n - 1)(p^2 - p) - \sum_{j=1}^{n-1} a_j(p - 1)) - (a_n(p - 1))
\]
\[
= (n - 1)(p^2 - p) - \left(\sum_{j=1}^{n} a_j\right)(p - 1)
\]
\[
= (n - 1)(p^2 - p) - ((n - 1)(p - 1)+1)(p - 1)
\]
\[
= (p - 1)(n - 2).
\]

Recall that if we choose the maximal \(b_j\)s, denoted \(B_j\), then \(B_j = p^2 - p - a_j(p - 1) = p(p - 1 - a_j) + a_j\). Note that this is the \(p\)-ary expansion of \(B_j\) since \(0 \leq a_j < p\), \(1 \leq j \leq n - 1\). We will have \([B_j/p] = p - 1 - a_j\) unless \(a_j = 0\). Without loss of generality assume \(a_1 = 0\). In order to have \(a_1 < p, a_{n-1} < p, a_n < p + 1, a_1 + \cdots + a_n = (n-1)(p - 1)+1\) and \(a_1 = 0\), we must have \(a_2 = p - 1, \ldots, a_{n-1} = p - 1\) and \(a_n = p\). In this case,

\[
\left(\begin{array}{c}
a_n(p - 1) \\
b_1, \ldots, b_{n-1}
\end{array}\right) = \left(\begin{array}{c}
p(p - 1) \\
p^2 - p, 0, \ldots, 0
\end{array}\right) \not\equiv 0 \mod p
\]

as desired. Now assume that all \(a_j \geq 1\). We still have \([B_j/p] = p - 1 - a_j\), and we may decrease each \(B_j\) by as much as \(a_j\) and still maintain the same value of
Recall that $B_1 + \cdots + B_p$ is too high by $(p-1)(n-2)$. We need to decrease the $B_j$'s by $(p-1)(n-2)$ in total while keeping $\sum_{i=1}^{n-1} [B_i/p] = a_n - 1$. Note that

$$
(p-1)(n-2) - \sum_{j=1}^{n-1} a_j = np - n - 2p + 2 - \sum_{j=1}^{n-1} a_j
$$

$$
= np - n - p + 2 - \sum_{j=1}^{n-1} a_j - p
$$

$$
= (n-1)(p-1) + 1 - \sum_{j=1}^{n-1} a_j - p
$$

$$
= a_n - p
$$

$$
\leq 0.
$$

Since $\sum_{j=1}^{n-1} a_j \geq (p-1)(n-2)$, we will be able to decrease each $B_j$ by no more than $a_j$ and still decrease the sum of the $B_j$'s by $(p-1)(n-2)$. As we have decreased at least one $B_j$ by at least one, we have also satisfied condition (3).

ACKNOWLEDGMENT

The author is grateful to the referee for several corrections, improvements in exposition and a more general statement of the main result.

REFERENCES

