PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 12, December 2012, Pages 4041–4052
S 0002-9939(2012)11310-3
Article electronically published on March 30, 2012

SMALL ZEROS OF QUADRATIC FORMS MOD P^2

TODD COCHRANE AND ALI H. HAKAMI

(Communicated by Matthew A. Papanikolas)

Abstract. Let $Q(\mathbf{x})$ be a quadratic form over $\mathbb{Z}$ in n variables, p be an odd prime and $\|\mathbf{x}\| = \max_i |x_i|$. A solution of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ is said to be nontrivial if $p \nmid x_i$ for some i. We prove that if this congruence has a nontrivial solution, then it has a nontrivial solution with $\|\mathbf{x}\| \leq p$. We also give estimates on the number of small nontrivial solutions of the congruence and show that there exists a set of n linearly independent nontrivial solutions of size $\|\mathbf{x}\| \leq (2^{n+1}+1)p$, provided that $n \geq 4$ is even and $Q(\mathbf{x})$ is nonsingular $\pmod p$.

1. Introduction

Let $Q = Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = \sum_{1\leq i \leq j \leq n} a_{ij}x_ix_j$ be a quadratic form with integer coefficients a_{ij}, m be a positive integer, and for any integer n-tuple $\mathbf{x}$, let $\|\mathbf{x}\| = \max |x_i|$. It is of interest to obtain small nonzero solutions of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{m}. \tag{1}$$

If $Q(\mathbf{x}) = x_1^2 + x_2^2 + \cdots + x_n^2$, then plainly any nonzero solution of (1) must have $\|\mathbf{x}\| \geq \frac{1}{\sqrt{n}} m^{1/2}$, and thus the goal in general is to obtain solutions with $\|\mathbf{x}\| \ll m^{1/2}$. Schinzel, Schlickewei and Schmidt [16] proved that (1) has a nonzero solution with

$$\|\mathbf{x}\| \leq \begin{cases} m^{\frac{1}{2}+\frac{1}{2n-2}}, & n \geq 2, \text{ even}, \\ m^{\frac{1}{2}+\frac{1}{2n}}, & n \geq 1, \text{ odd}. \end{cases} \tag{2}$$

This was sharpened by Heath-Brown [15] to

$$\|\mathbf{x}\| \ll \begin{cases} m^{\frac{13}{21}+\epsilon}, & n = 4,5, \\ m^{\frac{15}{26}+\epsilon}, & n = 6,7, \\ m^{\frac{6}{11}+\epsilon}, & n = 8,9, \\ m^{\frac{8}{15}+\epsilon}, & n = 10,11, \\ m^{\frac{1}{2}+\frac{3}{n^2}+\epsilon}, & n \geq 12, \text{ even}, \\ m^{\frac{1}{2}+\frac{3}{(n-1)^2}+\epsilon}, & n \geq 13, \text{ odd}. \end{cases} \tag{3}$$

It is also known [10] that for $n \geq 3$ there exists a constant c_Q depending on Q such that for any m there is a nonzero solution of (1) with $\|\mathbf{x}\| < c_Q m^{1/2}$.

Open problem 1. For $n \geq 4$ does there always exist a nonzero solution of (1) with $\|\mathbf{x}\| \leq m^{1/2}$?

Received by the editors January 26, 2011 and, in revised form, May 17, 2011.
2010 *Mathematics Subject Classification.* Primary 11D79, 11E08, 11H50, 11H55.
Key words and phrases. Quadratic forms, congruences, small solutions.

©2012 American Mathematical Society
Reverts to public domain 28 years from publication

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

The constant 1 in front of the $m^{1/2}$ (in the open problem) is sharp. Indeed, if $m = p^2$ with p a prime and λ is a quadratic nonresidue (mod p), then any nonzero solution of the congruence

$$x_1^2 - \lambda x_2^2 + p x_3^2 - \lambda p x_4^2 \equiv 0 \pmod{p^2} \tag{4}$$

must have $p | (x_1, x_2, x_3, x_4)$, that is, $\|\mathbf{x}\| \geq \sqrt{m}$.

For prime moduli $m = p$ it was established in a sequence of papers by Heath-Brown [14] and the first author [6], [7], [9] that the upper bound, $\|\mathbf{x}\| \ll p^{1/2}$, holds for $n \geq 4$. The best constant available is due to the second author [12, Theorem 1.3] who obtained the existence of a nonzero solution of (1) with

$$\|\mathbf{x}\| < \min\{p^{2/3}, 2^{19} p^{1/2}\},$$

for any $Q(\mathbf{x})$ in $n \geq 4$ variables. Wang [17], [18], [19] generalized this work to arbitrary finite fields. For $m = pq$ a product of two distinct primes, the optimal bound, $\|\mathbf{x}\| \ll m^{1/2}$ for $n \geq 4$, was obtained by the first author [8], [11], building upon the work of Heath-Brown [15].

If $n = 3$ the upper bound $m^{2/3}$ in (2) is best possible as noted by Heath-Brown [14]. To be precise, with $m = p$ a prime, $b = [p^{1/3}]$ and $Q(\mathbf{x}) = (x_2 - bx_1)^2 - \lambda(x_3 - b^2 x_1)^2$, where λ is a quadratic nonresidue (mod p), any nonzero solution of (1) has

$$\|\mathbf{x}\| \geq b^3/(b+1) > b(b-1) > m^{2/3} - 3m^{1/3}$$

(see [5, p. 17]). This quadratic form of course is degenerate. There remains

Open problem 2. For $n = 3$, and $m = p$ a prime, what is the smallest nonzero solution of (1) for any nondegenerate $Q(\mathbf{x})$ (mod p)?

Our interest in this paper is the case $m = p^2$ with p a prime. We seek small ($\|\mathbf{x}\| \ll p$) nontrivial solutions of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}. \tag{5}$$

This congruence has trivial small nonzero solutions such as $(p, 0, \dots, 0)$, and such solutions were allowable for the upper bounds in (2) and (3). Indeed, in the proofs of both (2) and (3), one writes $m = ab^2$ with a square-free, obtains a small solution (mod a) and then multiplies it by b to obtain a small solution (mod m). By nontrivial we shall mean a solution $\mathbf{x}$, with $p \nmid x_i$ for some i. For any such solution, if $\gcd(x_1, \dots, x_n) > 1$, then one can divide out this common factor to obtain a primitive solution of (5) of smaller size yet. By primitive we mean as usual a point with $\gcd(x_1, \dots, x_n) = 1$. Thus the existence of a small nontrivial solution of (5) is equivalent to the existence of a small primitive solution of (5).

As the example in (4) shows, when $n \leq 4$ there may not be any nontrivial solution of (5). We characterize all such forms in Lemma 3. When such a solution does exist, we find that there exists a nontrivial solution $\mathbf{x}$ with $\|\mathbf{x}\| \leq \sqrt{m}$.

Theorem 1. *Let $Q(\mathbf{x})$ be any quadratic form over $\mathbb{Z}$ in $n \geq 1$ variables and p be an odd prime. If the congruence (5) has a nontrivial solution, then it has a nontrivial solution with $\|\mathbf{x}\| \leq p$.*

The theorem does not generalize to higher prime powers without some further restrictions. For instance, the congruence

$$p^{k-1} x_1^2 + x_1 x_2 + p^{k-1} x_2^2 = (x_1 + p^{k-1} x_2)(x_2 + p^{k-1} x_1) \equiv 0 \pmod{p^k}$$

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

has primitive solutions $\pm(p^{k-1}, -1), \pm(-1, p^{k-1})$, and these are the smallest primitive solutions. Thus the minimal primitive solution is of size $m^{(k-1)/k}$. This example also shows that the upper bound in Theorem 1 is sharp (at least for $n = 2$). Theorem 1 improves on and generalizes a result of the second author, [13, Theorem 1], stating that for nonsingular $Q \pmod p$ in $n \geq 4$ variables, with n even, there exists a primitive solution of (5) with $\|\mathbf{x}\| \leq \max\{32p, 2^{18}\}$.

The proof of Theorem 1 is geometric, using the equivalence of quadratic forms, the construction of a lattice of solutions of (5), and the box principle, whereas the proof in [13] uses exponential sums. The method of exponential sums has the advantage that it allows us to give estimates on the number of small primitive solutions. We use this method to obtain the following lower bound.

Theorem 2. *Let $Q(\mathbf{x})$ be a quadratic form over $\mathbb{Z}$ in $n \geq 4$ variables with n even, and let p be an odd prime. If $Q(\mathbf{x})$ is nonsingular* (mod p)*, then the number N of nontrivial solutions of* (5) *with $\|\mathbf{x}\| < b$, where b is an odd multiple of p, $b < p^2/2$, satisfies $N > (.99)\frac{b^n}{p^2} - 10^n p^{n-2}$.*

In particular the theorem yields a nontrivial solution of (5) with $\|\mathbf{x}\| < 11p$. The theorem is stated in greater generality in Theorem 3, where we allow the box to have edges of different lengths. The proof here offers a number of simplifications and refinements of the method used in [13].

Theorem 2 implies the existence of a set of n linearly independent solutions of small size.

Corollary 1. *Under the hypotheses of Theorem* 2*, congruence* (5) *has a set of n primitive integer solutions $\mathbf{x}_1, \dots, \mathbf{x}_n$, linearly independent over $\mathbb{R}$, such that $\|\mathbf{x}_i\| \leq (2^{n+1} + 1)p$, $1 \leq i \leq n$.*

Remarks. 1. In order to simplify the proofs we have stated the lower bounds in Theorems 2 and 3 for boxes having edges of lengths that are multiples of p. In [12] and [13], weaker bounds of this type are given for boxes with sides of arbitrary lengths.

2. Our attempts to use the geometric method for congruences (mod p^3) (or higher powers) have not been successful in obtaining primitive solutions of size $\sqrt{m}$.

3. The method of exponential sums can be applied to any power of p and any n. In [12, Corollary 3.2] the second author obtained primitive solutions (mod p^3) with optimal bound $\|\mathbf{x}\| < 34\, p^{3/2}$ for any nonsingular quadratic form with $n \geq 6$ even, p sufficiently large and $\Delta = -1$, where Δ is as defined in (9). Weaker bounds are obtained for the case $\Delta = 1$. For a general prime power $m = p^k$ and nonsingular form (mod p^k) in $n \geq 4$ variables (n even), a primitive solution of size $\|\mathbf{x}\| \ll m^{\frac{1}{2}+\frac{1}{n}}$ was obtained in [12, Theorem 4.1].

4. An upper bound on the value N in Theorem 2 of the type $N \ll \frac{b^n}{p^2} + p^{n-1}$ can also be obtained by the methods here, but it is not optimal (one would like p^{n-1} replaced by p^{n-2}) due to our inability to obtain an optimal bound on the sum $\sum_{p^2|Q(\mathbf{y})} a(\mathbf{y})$ occurring in (11).

5. For a general modulus the problem of obtaining a small primitive solution remains unexplored. The correct answer will depend on the rank of the quadratic form modulo each of the prime divisors of m. For instance, the smallest primitive

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

solution of the congruence

$$p(x_1^2+x_2^2)+3p(x_3^2+x_4^2)+9(x_5^2-\lambda x_6^2)\equiv 0 \pmod{9p},$$

with $p>3$ a prime and λ a quadratic nonresidue (mod p) has size $\|\mathbf{x}\|=p$.

Open problem 3. If $n\geq 4$ and $Q(\mathbf{x})$ is nonsingular (mod p) for each prime divisor p of m, does (1) have a primitive solution of size $O(m^{1/2})$?

Notation. Throughout the paper we let $\mathbb{Z}_p$ denote the ring of p-adic integers and $\mathbb{Z}/(p^k)$ denote the ring of integers (mod p^k).

2. Review of quadratic forms

We start by reviewing some facts about quadratic forms. Let p^k be an odd prime power and $Q=Q(\mathbf{x})$ be a quadratic form with integer coefficients. Since p is odd and our concern is with congruences (mod p^k), we can bypass the subtleties that arise with $p=2$. In particular, we may assume that Q has a matrix representation $Q(\mathbf{x})=\mathbf{x}A_Q\mathbf{x}^t$, where A_Q is a symmetric matrix with integer entries. (Any $\frac{1}{2}$ that initially appears in the matrix may be replaced with a multiplicative inverse of 2 (mod p^k).) Q is said to be nonsingular or nondegenerate (mod p) if $p\nmid \det(A_Q)$. We will say that two forms Q_1 and Q_2 are equivalent (mod p^k), and write $Q_1\sim Q_2 \pmod{p^k}$ if there is a nonsingular linear transformation T (mod p^k) such that $Q_1(\mathbf{x})\equiv Q_2(T(\mathbf{x})) \pmod{p^k}$, that is, if there is an integer matrix P with $p\nmid\det(P)$ and $A_{Q_1}\equiv PA_{Q_2}P^t \pmod{p^k}$. Similarly, we say that Q_1 and Q_2 are equivalent over the p-adic integers $\mathbb{Z}_p$ if there exists an invertible matrix P over $\mathbb{Z}_p$ such that $A_{Q_1}=PA_{Q_2}P^t$. Clearly, if Q_1 and Q_2 are equivalent over $\mathbb{Z}_p$, then they are equivalent (mod p^k) for any k. Conversely, we deduce from Hensel's lemma the following.

Lemma 1. *If p is an odd prime and Q_1, Q_2 are quadratic forms over $\mathbb{Z}$ that are nonsingular* (mod p) *and equivalent* (mod p)*, then they are equivalent over the p-adic integers.*

Proof. We will just do the first step of the Hensel lifting, the general case being analogous. Suppose that Q_1 and Q_2 are equivalent nonsingular quadratic forms (mod p), with corresponding matrices A_{Q_1}, A_{Q_2}. Say $A_{Q_1}\equiv PA_{Q_2}P^t \pmod{p}$ for some integer matrix P, with P nonsingular (mod p). Replace P with $P+pT$, where T is a matrix of variables (to be solved for), and consider solving the congruence

$$A_{Q_1}\equiv (P+pT)A_{Q_2}(P+pT)^t \pmod{p^2}.$$

Letting $M=\frac{1}{p}(A_{Q_1}-PA_{Q_2}P^t)$, a matrix with integer entries, the preceding congruence may be written as

$$M\equiv TA_{Q_2}P^t+PA_{Q_2}T^t \pmod{p}.$$

Since M is symmetric, it suffices to solve the congruence $M\equiv 2TA_{Q_2}P^t \pmod{p}$, which is solvable since A_{Q_2} and P are nonsingular (mod p). Thus Q_1 and Q_2 are equivalent (mod p^2). □

Lemma 2. *Let p be an odd prime and $Q(\mathbf{x})$ be a quadratic form over $\mathbb{Z}$, nonsingular* (mod p)*, and having a nontrivial zero* (mod p)*. Then $Q\sim x_1x_2+a_3x_3^2+\cdots+a_nx_n^2$ over the p-adic integers, for some $a_i\in\mathbb{Z}$, $p\nmid a_i$, $3\leq i\leq n$ ($Q\sim x_1x_2$ for $n=2$).*

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Proof. By Lemma 1, it suffices to show that Q is equivalent to the desired form $\pmod{p}$, but this is well known for quadratic forms over fields. □

Next we characterize all quadratic forms having no nontrivial zero $\pmod{p^2}$. Let $Q(\mathbf{x})$ be a quadratic form in n variables over $\mathbb{Z}$, and let p be an odd prime. Then over the p-adic integers, Q is equivalent to a diagonal form (see, e.g., Cassels [4, Chapter 8]),

$$(6) \qquad Q \sim \sum_{i=1}^{n_1} a_i x_i^2 + p \sum_{i=n_1+1}^{n_1+n_2} a_i x_i^2 := Q_1 + pQ_2 \pmod{p^2},$$

say, for some $a_i \in \mathbb{Z}$, not divisible by p, $1 \le i \le n_1 + n_2$. The values n_1 and n_2 are uniquely determined. Q is degenerate $\pmod{p}$ if $n_1 < n$ and degenerate $\pmod{p^2}$ if $n_1 + n_2 < n$. If $n_1 \ge 3$, then Q_1 has a nontrivial zero $\pmod{p}$ and hence, by Hensel's Lemma, a nontrivial zero $\pmod{p^2}$. If $n_2 \ge 3$, then Q_2 has a nontrivial zero $\pmod{p}$. In either case, Q has a nontrivial zero $\pmod{p^2}$. If $Q_1 \sim a_1x_1^2 + a_2x_2^2$ or $Q_2 \sim a_1x_1^2 + a_2x_2^2$ with $(\frac{-a_1a_2}{p}) = 1$, then again Q has a nontrivial zero $\pmod{p^2}$. Finally, if Q is degenerate $\pmod{p^2}$, then it certainly has a nontrivial zero $\pmod{p^2}$. Thus we have

Lemma 3. *If $Q = Q(\mathbf{x})$ is a quadratic form in n variables over $\mathbb{Z}$ having no nontrivial zero $\pmod{p^2}$, then $n \le 4$ and Q is equivalent to one of the following types $\pmod{p^2}$. Here, a_1, a_2, a_3, a_4 denote integers not divisible by p.*

i) $n = 1$ and Q is not identically zero $\pmod{p^2}$.

ii) $n = 2$ and $Q \sim a_1x_1^2 + a_2x_2^2$ or $pa_1^2 + pa_2^2 \pmod{p^2}$ with $(\frac{-a_1a_2}{p}) = -1$ or $Q \sim a_1x_1^2 + pa_2x_2^2 \pmod{p^2}$.

iii) $n = 3$ and $Q \sim a_1x_1^2 + p(a_2x_2^2 + a_3x_3^2) \pmod{p^2}$ with $(\frac{-a_2a_3}{p}) = -1$ or $Q \sim a_1x_1^2 + a_2x_2^2 + pa_3x_3^2$ with $(\frac{-a_1a_2}{p}) = -1$.

iv) $n = 4$ and $Q \sim a_1x_1^2 + a_2x_2^2 + pa_3x_3^2 + pa_4x_4^2 \pmod{p^2}$, where both $(\frac{-a_1a_2}{p}) = -1$ and $(\frac{-a_3a_4}{p}) = -1$.

3. Proof of Theorem 1

The main tool in our proof is the following elementary result on the existence of small solutions to a system of linear congruences, the proof of which involves nothing more than the pigeon-hole principle, or what is commonly called the box principle. A proof and a discussion of its history and its many applications may be found in the work of Brauer and Reynolds [2].

Lemma 4. *Let $L_1(\mathbf{x}), \dots, L_k(\mathbf{x})$ be linear forms over $\mathbb{Z}$ in n variables and m be any positive integer. Then the system of congruences $L_i(\mathbf{x}) \equiv 0 \pmod{m}$, $1 \le i \le k$, has a nonzero solution $\mathbf{x}$ with $\|\mathbf{x}\| \le m^{k/n}$.*

Let $Q(\mathbf{x})$ be a quadratic form having a nontrivial zero $\pmod{p^2}$. If $Q(\mathbf{x})$ is degenerate $\pmod{p^2}$, then $Q \sim a_1x_1^2 + \cdots + a_rx_r^2 \pmod{p^2}$ for some $r < n$ and $a_i \in \mathbb{Z}$, $1 \le i \le r$, that is,

$$Q(\mathbf{x}) \equiv a_1L_1(\mathbf{x})^2 + \cdots + a_rL_r(\mathbf{x})^2 \pmod{p^2},$$

for some linear forms $L_i(\mathbf{x})$ over $\mathbb{Z}$, $1 \le i \le r$. By Lemma 4, the system $L_i(\mathbf{x}) \equiv 0 \pmod{p}$, $1 \le i \le r$, has a nonzero solution with $\|\mathbf{x}\| \le p^{r/n}$. Clearly, this is a nontrivial zero of $Q \pmod{p^2}$ with $\|\mathbf{x}\| < p$.

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Suppose now that Q is nondegenerate (mod p^2) and that it is equivalent (mod p^2) to a diagonal form of the type Q_1+pQ_2 (in the notation of (6)), where Q_1, Q_2 are nonsingular (mod p) quadratic forms in n_1, n_2 distinct variables with $n_1+n_2=n$. Let $\mathbf{x}$ be a nontrivial zero of Q_1+pQ_2 (mod p^2). Then either $p\nmid x_i$ for some $i\le n_1$, in which case Q_1 has a nontrivial zero (mod p), or $p|x_i$ for $1\le i\le n_1$, in which case Q_2 has a nontrivial zero (mod p). Thus, by Lemma 2, either Q_1 or Q_2 is equivalent (mod p^2) to a form of the type $x_1x_2+Q_3$ and thus so is Q, that is,

$$Q(\mathbf{x}) \equiv L_1(\mathbf{x})L_2(\mathbf{x}) + a_3L_3(\mathbf{x})^2 + a_4L_4(\mathbf{x})^2 + \cdots + a_nL_n(\mathbf{x})^2 \pmod{p^2},$$

for some linear forms L_i over $\mathbb{Z}$, $1\le i\le n$. In particular, any solution of the linear system $L_1(\mathbf{x})\equiv 0$ (mod p^2), $L_i(\mathbf{x})\equiv 0$ (mod p), $3\le i\le n$ satisfies $Q(\mathbf{x})\equiv 0$ (mod p^2). Theorem 1 now follows from the following lemma.

Lemma 5. *Let p be a prime and $L_1(\mathbf{x})$, $L_i(\mathbf{x})$, $3\le i\le n$, be linear forms in $\mathbf{x}=(x_1,x_2,\dots,x_n)$ over $\mathbb{Z}$ with $n\ge 2$. Then the system of congruences*

$$\begin{aligned} L_1(\mathbf{x}) &\equiv 0 \pmod{p^2}, \\ L_i(\mathbf{x}) &\equiv 0 \pmod{p}, \quad 3\le i\le n, \end{aligned} \tag{7}$$

has a primitive solution with $\|\mathbf{x}\|\le p$. (If $n=2$, the system is just $L_1(\mathbf{x})\equiv 0$ (mod p^2).)

Proof. Let $L_1(\mathbf{x}) = c_1x_1+c_2x_2+\cdots+c_nx_n$. We claim that by the box principle the system (7) has a nonzero solution $\mathbf{x}$ with

$$|x_i|<p, \qquad 1\le i\le n-1, \qquad |x_n|\le p. \tag{8}$$

Indeed, letting the x_i run through the values $0\le x_i\le p-1$, $1\le i\le n-1$, $0\le x_n\le p$, there are $p^{n-1}(p+1)>p^n$ choices for $\mathbf{x}$, and so at least two of the $(n-1)$-tuples $(L_1(\mathbf{x}),L_3(\mathbf{x}),\dots,L_n(\mathbf{x}))\in \mathbb{Z}/(p^2)\times\mathbb{Z}/(p)\times\cdots\times\mathbb{Z}/(p)$ must be equal, say for $\mathbf{x}\ne\mathbf{y}$. The desired solution is then $\mathbf{x}-\mathbf{y}$.

Let $\mathbf{x}$ be a nonzero solution of (7) satisfying (8). If $p\nmid x_i$ for some i we are done (that is, $\mathbf{x}$ is a primitive solution with $\|\mathbf{x}\|\le p$). If $p|x_i$ for all i, then $x_i=0$, $1\le i\le n-1$ (since $|x_i|<p$) and $x_n=\pm p$ (so that $\mathbf{x}\ne\mathbf{0}$). But then the congruence $L_1(\mathbf{x})\equiv 0$ (mod p^2) implies that $p|c_n$. In a similar manner, for $1\le i\le n-1$ we obtain a small primitive solution unless $p|c_i$. Thus we are left with the case where p divides all of the coefficients of L_1. In this case put $L_1'(\mathbf{x}) := \frac{1}{p}L_1(\mathbf{x})$, a linear form with integer coefficients. Then system (7) is equivalent to the system $L_1'(\mathbf{x})\equiv L_i(\mathbf{x})\equiv 0$ (mod p), $3\le i\le n$. But by Lemma 4 the latter system has a nonzero solution $\mathbf{x}$ with $\|\mathbf{x}\|<p^{(n-1)/n}$. □

4. The method of exponential sums

The proof of Theorem 2 follows closely the method of the second author [13], and so we shall omit some of the details here and focus on the essential refinements of [13]. We abbreviate complete sums over $(\mathbb{Z}/(p^2))^n$ and $(\mathbb{Z}/(p))^n$ in the manner

$$\sum_{\mathbf{x}} = \sum_{\mathbf{x}\ (p^2)} = \sum_{x_1=1}^{p^2}\cdots\sum_{x_n=1}^{p^2}, \qquad \sum_{\mathbf{x}\ (p)} = \sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}.$$

It is also convenient to write $p|\mathbf{y}$ to mean $p|y_i$ for $1\le i\le n$.

Let $Q(\mathbf{x}) = \mathbf{x}A_Q\mathbf{x}^t$ be a quadratic form in n variables with A_Q a symmetric matrix over $\mathbb{Z}$ and p an odd prime. For the purpose of this paper we shall assume

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

that Q is nonsingular (mod p) and that n is even, although the method applies as well to any Q. Set

$$\Delta = \Delta_p(Q) = \left(\frac{(-1)^{n/2}\det A_Q}{p}\right), \tag{9}$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol. It is well known that $Q \sim x_1x_2 + x_2x_4 + \cdots + x_{n-1}x_n \pmod p$ if and only if $\Delta_p(Q) = 1$, and thus it is plain that the value of $\Delta_p(Q)$ plays an important role in the distribution of the zeros of Q. Let $V = V_{p^2}(Q)$ be the set of zeros of Q contained in $(\mathbb{Z}/(p^2))^n$ and V^* the set of points in V that are nonzero (mod p). We call V^* the set of primitive zeros of $Q \pmod{p^2}$. These points correspond to the nontrivial solutions of (5).

For $\mathbf{y} \in \mathbb{Z}^n$, set

$$\phi(V,\mathbf{y}) = \begin{cases} \sum\limits_{\mathbf{x}\in V} e_{p^2}(\mathbf{x}\cdot\mathbf{y}) & \text{for } \mathbf{y} \not\equiv \mathbf{0} \pmod{p^2}, \\ |V| - p^{2(n-1)} & \text{for } \mathbf{y} \equiv \mathbf{0} \pmod{p^2}, \end{cases}$$

where $e_{p^2}(\cdot) = e^{\frac{2\pi i \cdot}{p^2}}$ and $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^n x_iy_i$, viewing $\mathbb{Z}/(p^2)$ as a $\mathbb{Z}$-module. Also, let Q^* denote the quadratic form associated with A_Q^{-1}, a matrix with integer entries that is a multiplicative inverse of $A_Q \pmod{p^2}$. Using standard formulae for quadratic Gauss sums one obtains ([12, Lemma 2.3]),

Lemma 6. *Suppose n is even, Q is nonsingular* (mod p) *and $\Delta = \Delta_p(Q)$. For $\mathbf{y} \in \mathbb{Z}^n$, put $\mathbf{y}' = \frac{1}{p}\mathbf{y}$ in case $p|\mathbf{y}$. Then for any $\mathbf{y}$,*

$$\phi(V,\mathbf{y}) = \begin{cases} p^n - p^{n-1} & \text{if } p \nmid \mathbf{y} \text{ and } p^2|Q^*(\mathbf{y}), \\ -p^{n-1} & \text{if } p \nmid \mathbf{y} \text{ and } p\|Q^*(\mathbf{y}), \\ 0 & \text{if } p \nmid \mathbf{y} \text{ and } p \nmid Q^*(\mathbf{y}), \\ -\Delta p^{3n/2-2} + p^{n-1}(p-1) & \text{if } p|\mathbf{y} \text{ and } p \nmid Q^*(\mathbf{y}'), \\ \Delta(p-1)p^{3n/2-2} + p^{n-1}(p-1) & \text{if } p|\mathbf{y} \text{ and } p\ |Q^*(\mathbf{y}'). \end{cases}$$

When $\mathbf{y} = \mathbf{0}$, Lemma 6 gives the cardinality of V,

$$|V| = p^{2n-2} + \Delta(p-1)p^{\frac{3n}{2}-2} + p^{n-1}(p-1).$$

5. Fundamental identity

Let $\alpha(\mathbf{x})$ be a complex-valued function defined on $(\mathbb{Z}/(p^2))^n$ with Fourier expansion

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})e_{p^2}(\mathbf{y}\cdot\mathbf{x}), \tag{10}$$

where

$$a(\mathbf{y}) = p^{-2n}\sum_{\mathbf{x}} \alpha(\mathbf{x})e_{p^2}(-\mathbf{x}\cdot\mathbf{y}).$$

(Again, unless indicated otherwise, the sums throughout this section are complete sums over $\mathbb{Z}/(p^2)$.) In particular, $a(\mathbf{0}) = p^{-2n}\sum_{\mathbf{x}}\alpha(\mathbf{x})$. By [12, Lemma 2.4], we have

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Proposition 1 (**Fundamental identity**). *Let $n \geq 2$ be even, Q be a nonsingular quadratic form* (mod p) *in n variables, and V^* be the set of primitive zeros of Q* (mod p^2). *Then for any $\alpha(\mathbf{x})$ we have*

$$\sum_{\mathbf{x}\in V^*} \alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1} \sum_{p|Q^*(\mathbf{y})} a(\mathbf{y})$$
$$- \left(\Delta p^{\frac{3n}{2}-2} + p^n\right) \sum_{\mathbf{y}'\ (p)} a(p\mathbf{y}') + \Delta p^{\frac{3n}{2}-1} \sum_{\substack{\mathbf{y}'\ (p)\\ p|Q^*(\mathbf{y}')}} a(p\mathbf{y}').$$

The identity simplifies if α is chosen so that its Fourier coefficients vanish whenever $p|\mathbf{y}$, $\mathbf{y} \neq \mathbf{0}$. For any such α, using $a(\mathbf{0}) = p^{-2n}\sum_{\mathbf{x}} \alpha(\mathbf{x})$, we have

$$\sum_{\mathbf{x}\in V^*} \alpha(\mathbf{x}) = p^{-2}\delta_p \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1} \sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}), \tag{11}$$

where

$$\delta_p = \left(1 + \Delta p^{-n/2}(p-1) - p^{-n+2}\right), \tag{12}$$

a positive value (close to 1) unless $n = 2$ and $\Delta = -1$, the case where V^* is empty. This observation allows us to greatly simply the proofs in [12] and [13].

6. Proof of Theorem 2

Let $\mathcal{B}$ be a box of points centered about the origin,

$$\mathcal{B} = \{\mathbf{x} : |x_i| < m_i/2, 1 \leq i \leq n\} \subseteq (\mathbb{Z}/(p^2))^n, \tag{13}$$

with the m_i multiples of p, $m_i \leq p^2$, $1 \leq i \leq n$. For convenience, we often insist further that the m_i be odd so that we have $|\mathcal{B}| = \prod_{i=1}^n m_i$. The characteristic function $\chi_{\mathcal{B}}$ for $\mathcal{B}$ has Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y}) e_{p^2}(\mathbf{y}\cdot\mathbf{x})$, with

$$a_{\mathcal{B}}(\mathbf{y}) = p^{-2n} \prod_{i=1}^n \frac{\sin(\pi m_i y_i/p^2)}{\sin(\pi y_i/p^2)}, \tag{14}$$

where the term in the product is understood to be m_i when $y_i = 0$. By imposing the constraint that $p|m_i$ for all i, we see that $a_{\mathcal{B}}(\mathbf{y}) = 0$ if $p|\mathbf{y}$, unless $\mathbf{y} = \mathbf{0}$.

Let $\alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}$. Then α is supported on $\mathcal{B} + \mathcal{B}$, and its Fourier coefficients $a(\mathbf{y}) = p^{2n} a_{\mathcal{B}}^2(\mathbf{y})$ also satisfy $a(\mathbf{y}) = 0$ if $p|\mathbf{y}$, $\mathbf{y} \neq \mathbf{0}$. Since $\sum_{\mathbf{x}} \alpha(\mathbf{x}) = |\mathcal{B}|^2$ and

$$\sum_{\mathbf{x}\in \mathbb{V}^*} \alpha(\mathbf{x}) \leq |\mathcal{B}||V^* \cap (\mathcal{B}+\mathcal{B})|,$$

we obtain from (11),

Lemma 7. *Let $n \geq 2$ be even, Q be nonsingular* (mod p) *and V^* be the set of primitive zeros of Q* (mod p^2). *For any box $\mathcal{B}$ of type* (13) *with the m_i all multiples of p we have*

$$|V^* \cap (\mathcal{B}+\mathcal{B})| \geq \frac{\delta_p|\mathcal{B}|}{p^2} - \frac{p^{n-1}}{|\mathcal{B}|} \sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}). \tag{15}$$

We are left with estimating $\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y})$.

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Lemma 8. *Let $n \geq 2$ be even and Q be nonsingular* (mod p). *For any box $\mathcal{B}$ of type* (13) *with $7p \leq m_i < p^2$, m_i odd, $1 \leq i \leq n$,*

$$\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) \leq \begin{cases} 11^n \frac{|\mathcal{B}|}{p} + 3^n \frac{|\mathcal{B}|^2}{p^{\frac{3}{2}n+1}} & \text{if } \Delta = -1, \\ 11^n \frac{|\mathcal{B}|}{p} + 3^n \frac{|\mathcal{B}|^2}{p^{\frac{3}{2}n}} & \text{if } \Delta = 1, \end{cases}$$

where the $a(\mathbf{y})$ are the Fourier coefficients of $\alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}$. If $\mathcal{B}$ is a cube, then the 11 *can be replaced by* 10.

Proof. Write $\mathbf{y} = \mathbf{u} + p\mathbf{v}$ with $\mathbf{u}, \mathbf{v}$ running through complete residue systems (mod p), $|u_i| < p/2$, $|v_i| < p/2$, so that by (14),

$$\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) = p^{-2n} \sum_{p|Q^*(\mathbf{u})} \prod_{i=1}^{n} \sum_{|v_i|<p/2} \frac{\sin^2(\pi m_i(u_i + pv_i)/p^2)}{\sin^2(\pi(u_i + pv_i)/p^2)}.$$

Using $|\sin(\pi x)| > 2|x|$ for $|x| < 1/2$, we have

$$\begin{aligned} \sum_{|v_i|<p/2} \frac{\sin^2(\pi m_i(u_i + pv_i)/p^2)}{\sin^2(\pi(u_i + pv_i)/p^2)} &= \frac{\sin^2(\pi m_i u_i/p^2)}{\sin^2(\pi u_i/p^2)} \\ &\quad + \sum_{0<|v_i|<p/2} \frac{\sin^2(\pi m_i(u_i + pv_i)/p^2)}{\sin^2(\pi(u_i + pv_i)/p^2)} \\ &\leq \min\left\{m_i^2, \frac{p^4}{4u_i^2}\right\} + \frac{p^4}{4} \sum_{v_i=1}^{\infty} \frac{1}{(u_i + pv_i)^2} \\ &\quad + \frac{1}{(u_i - pv_i)^2} \\ &\leq \min\left\{m_i^2, \frac{p^4}{4u_i^2}\right\} + p^2\left(\frac{\pi^2}{4} - 1\right), \end{aligned}$$

the latter inequality following from the fact that the infinite series is maximized at $u_i = p/2$ (since for any fixed $v \geq 1$, the function $f(u) = (u + pv)^{-2} + (u - pv)^{-2}$ is even and monotone increasing on $[0, p/2]$). Using $\pi^2/4 - 1 < 3/2$, we conclude

$$\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) < p^{-2n} \sum_{p|Q^*(\mathbf{u})} \prod_{i=1}^{n} \min\left(m_i^2 + \frac{3}{2}p^2, \frac{p^4}{4u_i^2} + \frac{3}{2}p^2\right). \tag{16}$$

To complete the proof, one partitions the set of $\mathbf{u}$ into dyadic boxes and uses an upper bound [9] on the number of zeros of Q^* in a box; see [12] or [13]. □

Theorem 2 is a special case of the following theorem.

Theorem 3. *Let $n \geq 4$ be even, Q be nonsingular* (mod p) *and V^* be the set of primitive zeros of Q* (mod p^2). *For any box $\mathcal{B}$ of type* (13) *with m_i odd, $p|m_i$, $7p \leq m_i \leq p^2$, $1 \leq i \leq n$, we have*

$$|V^* \cap (\mathcal{B} + \mathcal{B})| \geq \delta_p' \frac{|\mathcal{B}|}{p^2} - 11^n p^{n-2}, \tag{17}$$

where

$$\delta_p' = \begin{cases} 1 - \frac{(p-1)}{p^{\frac{n}{2}}} - \frac{1}{p^{n-2}} - \frac{3^n}{p^{\frac{n}{2}}}, & \text{if } \Delta = -1, \\ 1 + \frac{(p-1)}{p^{\frac{n}{2}}} - \frac{1}{p^{n-2}} - \frac{3^n}{p^{\frac{n}{2}-1}}, & \text{if } \Delta = 1. \end{cases}$$

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

For any cube $\mathcal{B}$ symmetric about the origin, with edges of length λp, $\lambda \le p/2$, λ odd, we have

$$|V^* \cap (\mathcal{B}+\mathcal{B})| \ge (.99)\frac{|\mathcal{B}|}{p^2} - 10^n p^{n-2}. \tag{18}$$

One can compare the results of [13, Theorem 3, Theorem 5], where it is shown that for $|\mathcal{B}| \ge 2^{4n+3}p^n$ and $m_i \ge p$, $1 \le i \le n$, $|V \cap (\mathcal{B}+\mathcal{B})| > \frac{|\mathcal{B}|}{4p^2}$.

Proof. By Lemma 7 and Lemma 8 we have for $\Delta = -1$,

$$|V^* \cap (\mathcal{B}+\mathcal{B})| \ge \frac{\delta_p|\mathcal{B}|}{p^2} - \frac{p^{n-1}}{|\mathcal{B}|}\left(11^n\frac{|\mathcal{B}|}{p} + 3^n\frac{|\mathcal{B}|^2}{p^{\frac{3}{2}n+1}}\right), \tag{19}$$

and the result follows. A similar argument holds for $\Delta = 1$. The result for cubes is just a calculation. □

7. Proof of Corollary 1

For any n-tuple $\mathbf{a}$ of integers with $p \nmid \mathbf{a}$, let $H(\mathbf{a})$ denote the hyperplane

$$H(\mathbf{a}) := \{\mathbf{x} \in (\mathbb{Z}/(p^2))^n : \sum_{i=1}^n a_i x_i \equiv 0 \pmod{p^2}\}.$$

Corollary 1 is an easy consequence of

Corollary 2. *Let Q be a nonsingular quadratic form* (mod p) *in an even number of variables $n \ge 4$. Then for any hyperplane $H(\mathbf{a})$ with $p \nmid \mathbf{a}$, there is a primitive solution of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$, not on the hyperplane, with $\|x\| < (2^{n+1}+1)p$.*

Proof. Let $\mathcal{B}$ be a box of type (13) with $m_i = \lambda p$, $1 \le i \le n$, λ odd. Say $p \nmid a_n$ and that $H(\mathbf{a})$ is given by the congruence $x_n \equiv a_1' x_1 + \cdots + a_{n-1}' x_{n-1} \pmod{p^2}$, so that the number of points in $V \cap H(\mathbf{a}) \cap (\mathcal{B}+\mathcal{B})$ is at most the number of integer solutions of the congruence

$$Q_{\mathbf{a}}(x_1,\dots,x_{n-1}) := Q(x_1,\dots,x_{n-1}, a_1'x_1 + \cdots + a_{n-1}'x_{n-1}) \equiv 0 \pmod{p^2},$$

with $|x_i| < \lambda p$, $1 \le i \le n-1$. This number is certainly no more than the number of integer solutions of the congruence $Q_{\mathbf{a}}(x_1,\dots,x_{n-1}) \equiv 0 \pmod{p}$, with $|x_i| < \lambda p$, which is at most $(2\lambda)^{n-1}|V_p|$, where V_p is the full set of zeros of $Q_{\mathbf{a}}$ (mod p). Since Q is nonsingular (mod p), $Q_{\mathbf{a}}$ is of rank $n-1$ or $n-2$. In the former case $|V_p| = p^{n-2}$, and in the latter case, $|V_p| = p^{n-2} \pm (p-1)p^{\frac{n}{2}-1}$; see, e.g., [1, Section 1.3]. Thus

$$|V \cap H(\mathbf{a}) \cap (\mathcal{B}+\mathcal{B})| \le (2\lambda)^{n-1}\left(p^{n-2} + p^{\frac{n}{2}}\right) \le 2^n\lambda^{n-1}p^{n-2}.$$

On the other hand, by (18), for any odd $\lambda < p/2$,

$$|V^* \cap (\mathcal{B}+\mathcal{B})| > ((.99)\lambda^n - 10^n)\,p^{n-2}.$$

If $\lambda \ge 2^{n+1}$, then $2^n\lambda^{n-1} < (.99)\lambda^n - 10^n$ for $n \ge 4$. Taking $\lambda = 2^{n+1}+1$ (to make it odd) completes the proof. (Note, if $2^{n+1}+1 > p/2$, the result is trivial since V^* always contains a point not on $H(\mathbf{a})$.) □

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Proof of Corollary 1. The proof is by contradiction. Suppose that there does not exist a set of n linearly independent (over $\mathbb{R}$) primitive integer solutions of $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ with $\|\mathbf{x}\| < (2^{n+1}+1)p$. Then all such solutions of this congruence must lie on a hyperplane, and moreover the hyperplane can be defined by an equation of the type $\sum_{i=1}^{n} a_i x_i = 0$, with $a_i \in \mathbb{Z}$, $1 \leq i \leq n$, and $\gcd(a_1, \ldots, a_n) = 1$. In particular, their residues $\pmod{p^2}$ all belong to $H(\mathbf{a})$, contradicting Corollary 2. □

Acknowledgement

The first author wishes to express his thanks to the Department of Mathematics at Georgia Institute of Technology, where he was visiting during the preparation of part of this work.

References

[1] Z. I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, Vol. 20 in Series on Pure and Applied Mathematics, New York, 1966. MR0195803 (33:4001)

[2] A. Brauer and R.L. Reynolds, *On a theorem of Aubry-Thue*, Canadian J. Math. 3 (1951), 367-374. MR0048487 (14:21a)

[3] L. Carlitz, *Weighted quadratic partitions* (mod p^r), Math Zeit. 59 (1953), 40-46. MR0061118 (15:777c)

[4] J. W. S. Cassels, *Rational quadratic forms,* London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR522835 (80m:10019)

[5] T. Cochrane, *Small solutions of congruences*, Ph.D. Thesis, The University of Michigan, 1984. MR2633623

[6] ———, *Small zeros of quadratic forms modulo p*, J. Number Theory 33 (1989), no. 3, 286-292. MR1027056 (90k:11034)

[7] ———, *Small zeros of quadratic forms modulo p, II*, Proceedings of the Illinois Number Theory Conference of 1989, Birkhäuser, Boston (1990), 91-94. MR1084175 (92d:11027)

[8] ———, *Small zeros of quadratic congruences modulo pq,* Mathematika 37 (1990), no. 2, 261-272. MR1099775 (92d:11029)

[9] ———, *Small zeros of quadratic forms modulo p, III*, J. Number Theory 37 (1991), no. 1, 92-99. MR1089791 (92d:11028)

[10] ———, *On representing the multiple of a number by a quadratic form*, Acta Arith. 63 (1993), no. 3, 211-222. MR1218236 (94c:11032)

[11] ———, *Small zeros of quadratic congruences modulo pq, II*, J. Number Theory 50 (1995), no. 2, 299-308. MR1316824 (95m:11036)

[12] A. H. Hakami, *Small zeros of quadratic congruences to prime power moduli*, Ph.D. Thesis, 2009.

[13] ———, *Small zeros of quadratic forms modulo* p^2, JP J. Algebra, Number Theory and Applications, 17 (2010), no. 2, 141-162. MR2742255

[14] D.R. Heath-Brown, *Small solutions of quadratic congruences*, Glasgow Math. J. 27 (1985), 87-93. MR819830 (87i:11042)

[15] ———, *Small solutions of quadratic congruences, II,* Mathematika 38 (1991), no. 2, 264-284. MR1147826 (93d:11039)

[16] A. Schinzel, H.P. Schlickewei and W.M. Schmidt, *Small solutions of quadratic congruences and small fractional parts of quadratic forms*, Acta Arithmetica 37 (1980), 241-248. MR598879 (81m:10063)

[17] Y. Wang, *On small zeros of quadratic forms over finite fields*, Algebraic structures and number theory (Hong Kong, 1988), 269–274, World Sci. Publ., Teaneck, NJ, 1990. MR1098057 (92c:11030)

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

[18] ______, *On small zeros of quadratic forms over finite fields*, J. Number Theory, 31 (1989), 272-284. MR993904 (90c:11022)

[19] ______, *On small zeros of quadratic forms over finite fields. II.* A Chinese summary appears in Acta Math. Sinica 37 (1994), no. 5, 719-720. Acta Math. Sinica (N.S.) 9 (1993), no. 4, 382-389. MR1380091 (97a:11055)

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506
E-mail address: `cochrane@math.ksu.edu`

Department of Mathematics, King Khalid University, Abha, Saudi Arabia 61431
E-mail address: `aalhakami@kku.edu.sa`

Licensed to Kansas State University. Prepared on Fri Nov 2 11:13:27 EDT 2012 for download from IP 129.130.36.167.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use