QUADRATIC EQUATIONS WITH FIVE PRIME UNKNOWNS

STEPHEN KWOK-KWONG CHOI AND ANGEL V. KUMCHEV

1. Introduction

Let n be an integer and let $b_1, \dots, b_5$ be non-zero integers. In this paper, we consider the quadratic equation

$$b_1 p_1^2 + \cdots + b_5 p_5^2 = n, \tag{1.1}$$

where $p_1, \dots, p_5$ are prime unknowns. In order to avoid degenerate cases, we need to impose certain local conditions. For example, unless

$$b_1 + \cdots + b_5 \equiv n \pmod{24}, \tag{1.2}$$

every solution $p_1, \dots, p_5$ of (1.1) must contain the primes 2 and 3. Further conditions arise from primes dividing three or more of the coefficients (see [1, §6]). For our purposes, it suffices to say that the hypotheses of Theorem 1 below preclude degeneracies from occurring. Our goal is to prove the existence of solutions of (1.1) that do not grow too rapidly as $\max\{|b_1|, \dots, |b_5|\} \to \infty$. The main result of the paper is the following theorem.

Theorem 1. *Let $b_1, \dots, b_5$ be non-zero integers satisfying*

$$\gcd(b_i, b_j, b_k) = 1, \quad 1 \le i < j < k \le 5 \tag{1.3}$$

and

$$|b_1| \ge \cdots \ge |b_5|, \tag{1.4}$$

and let n be an integer satisfying (1.2)*. Also, suppose that* 5 *divides at most two of the numbers $b_1, \dots, b_5, n$. If $b_1, \dots, b_5$ are not all of the same sign, then* (1.1) *is soluble in primes $p_1, \dots, p_5$ satisfying*

$$p_j \ll \sqrt{|n|} + |b_1 \cdots b_4|^{2+\varepsilon}. \tag{1.5}$$

If $b_1, \dots, b_5$ are all positive, then (1.1) *is soluble provided that*

$$n \gg b_5 (b_1 \cdots b_4)^{4+\varepsilon}. \tag{1.6}$$

The implied constants in (1.5) *and* (1.6) *depend only on ε.*

This result improves on earlier work by M. C. Liu and Tsang [5] and by the first author and J. Y. Liu [1, 2]. M. C. Liu and Tsang obtained a variant of Theorem 1, in which (1.5) and (1.6) are replaced by the bounds

$$p_j \ll \sqrt{|n|} + \max\{|b_1|, \dots, |b_5|\}^A \tag{1.7}$$

and

$$n \gg \max\{b_1, \dots, b_5\}^A, \tag{1.8}$$

Date: September 14, 2015.

Research of Stephen Choi was supported by NSERC of Canada.

where A is an absolute constant. Their method is similar to the approach used by Montgomery and Vaughan [6] to estimate the cardinality of the exceptional set in Goldbach's problem. In [1, 2], Choi and J. Y. Liu used a different method to prove (1.7) and (1.8) with $A = 25/2$ and $A = 26$, respectively, under the more stringent hypothesis that the coefficients $b_1, \dots, b_5$ are pairwise coprime.

It is natural to ask whether one can improve further on Theorem 1, and if so, then by how much. While we do not know what the best possible result should be, it is not difficult to produce lower bounds for the exponents in (1.7) and (1.8). Indeed, when all the b_j's are positive the inequality $n \geq b_1$ is obviously a necessary condition for the solubility of (1.1). Similarly, if $|b_1|$ is sufficiently large, $n = o(|b_1|)$, and $b_2, \dots, b_5$ are bounded, then (1.1) has no solution in prime numbers $p_1, \dots, p_5$ subject to

$$p_j \ll \sqrt{|n|} + o(\sqrt{|b_1|}).$$

Therefore, at least in the favorable case when $b_2, \dots, b_5$ are bounded above by an absolute constant, the exponents 2 and 4 in (1.5) and (1.6) are within a factor of (at most) 4 from the best possible exponents.

Theorem 1 is even closer to the limit of the methods employed in its proof. As in earlier work, since our main tool is the Hardy–Littlewood circle method, the strength of our results is determined by certain estimates for Weyl sums over primes. Even if we were to assume that those exponential sums satisfy "fantastic" bounds, far beyond those we can establish, it is inherent to the circle method that it cannot yield (1.5) with exponent $1/2$ in place of $2+\varepsilon$ or (1.6) with exponent 1 in place of $4 + \varepsilon$. Theorem 1 relies on the estimates obtained recently by the second author [3] (see Lemma 2.1 below).

Notation. Throughout the paper, the letter p, with or without subscripts, is reserved for prime numbers; the letter c denotes an absolute constant, not necessarily the same in all occurrences. As usual in number theory, $\phi(n)$ and $\omega(n)$ denote Euler's totient function and the number of distinct prime divisors of n. We also write $e(x) = e^{2\pi i x}$, $e_q(x) = e(x/q)$, $[a, \dots, b] = \operatorname{lcm}[a, \dots, b]$, and $(a, \dots, b) = \gcd(a, \dots, b)$.

2. Preliminaries

We first derive estimates for the generating functions appearing in the proof from estimates for the exponential sum

$$S(\alpha) = \sum_{X < p \leq 2X} (\log p) e\left(\alpha p^2\right). \tag{2.1}$$

We start by quoting two results of the second author [3].

Lemma 2.1. *Let $S(\alpha)$ be defined by (2.1), and suppose that $a \in \mathbb{Z}$, $q \in \mathbb{N}$, and $(a, q) = 1$. For any fixed $\varepsilon > 0$, we have*

$$S(\alpha) \ll X^{11/20+\varepsilon} \Psi(\alpha)^{1/2} + X^{1+\varepsilon} \Psi(\alpha)^{-1/2}, \tag{2.2}$$

where $\Psi(\alpha) = q + X^2 |q\alpha - a|$. Furthermore, if

$$1 \leq q \leq X^{3/2} \quad \text{and} \quad |q\alpha - a| \leq X^{-3/2},$$

we have

$$S(\alpha) \ll X^{7/8+\varepsilon} + X^{1+\varepsilon} \Psi(\alpha)^{-1/2}. \tag{2.3}$$

Proof. (2.2) is the case $k = 2$ of [3, Theorem 2], and (2.3) is the case $k = 2$ of [3, Theorem 3]. □

The next two lemmas generalize (2.2) and (2.3) to $S(b\alpha)$, with b a non-zero integer.

Lemma 2.2. *Let b be a non-zero integer and let $S(\alpha)$ be defined by (2.1). Suppose that there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfying*

$$1 \le q \le P, \quad (a,q) = 1, \quad |q\alpha - a| < P/(|b|X^2), \tag{2.4}$$

with $P < \frac{1}{2}X$. Then, for any fixed $\varepsilon > 0$, we have

$$S(b\alpha) \ll X^{11/20+\varepsilon}\Phi(\alpha)^{1/2} + X^{1+\varepsilon}\Phi(\alpha)^{-1/2}, \tag{2.5}$$

where $\Phi(\alpha) = q_1\left(1 + |b|X^2|\alpha - a/q|\right)$ and $q_1 = q/(b,q)$.

Proof. By Dirichlet's theorem on diophantine approximation, there exist integers a_1 and q_1 satisfying

$$1 \le q_1 \le X, \quad (a_1,q_1) = 1, \quad |q_1 b\alpha - a_1| < X^{-1}. \tag{2.6}$$

Combining (2.4) and (2.6), we obtain

$$|q_1 ba - qa_1| \le q_1|b||q\alpha - a| + q|q_1 b\alpha - a_1| \le 2PX^{-1} < 1,$$

and hence

$$\frac{a_1}{q_1} = \frac{ab}{q} \quad \text{and} \quad q_1 = \frac{q}{(q,b)}.$$

Thus

$$\Phi(\alpha) = q_1 + X^2|q_1 b\alpha - a_1|,$$

and the lemma follows from (2.2) with $\alpha = b\alpha$, $q = q_1$, and $a = a_1$. □

Lemma 2.3. *Let b be a non-zero integer and let $S(\alpha)$ be defined by (2.1). Suppose that there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfying*

$$1 \le q \le |b|X^2P^{-1}, \quad (a,q) = 1, \quad |q\alpha - a| < P/(|b|X^2), \tag{2.7}$$

with P subject to

$$2|b|X^{1/4} < P \le X. \tag{2.8}$$

Then, for any fixed $\varepsilon > 0$, we have

$$S(b\alpha) \ll X^{7/8+\varepsilon} + X^{1+\varepsilon}\Phi(\alpha)^{-1/2}, \tag{2.9}$$

where $\Phi(\alpha) = q_1\left(1 + |b|X^2|\alpha - a/q|\right)$ and $q_1 = q/(b,q)$.

Proof. By Dirichlet's theorem, there exist integers a_1 and q_1 such that

$$1 \le q_1 \le X^{3/2}, \quad (a_1,q_1) = 1, \quad |q_1 b\alpha - a_1| < X^{-3/2}.$$

Hence, by (2.3) with $\alpha = b\alpha$, $q = q_1$, and $a = a_1$,

$$S(b\alpha) \ll X^{7/8+\varepsilon} + \frac{X^{1+\varepsilon}}{(q_1 + X^2|q_1 b\alpha - a_1|)^{1/2}}. \tag{2.10}$$

If $q_1 > X^{1/4}$ or $|q_1 b\alpha - a_1| > X^{-7/4}$, the first term on the right side of (2.10) dominates the second and (2.9) follows. Otherwise, recalling (2.7) and (2.8), we get

$$\begin{aligned} |q_1 ba - aq_1| &\le q_1|b||q\alpha - a| + q|q_1 b\alpha - a_1| \\ &\le PX^{-7/4} + |b|X^{1/4}P^{-1} < 1. \end{aligned}$$

Thus

$$\frac{a_1}{q_1} = \frac{ab}{q} \quad \text{and} \quad q_1 = \frac{q}{(q,b)},$$

and (2.10) turns into (2.9). □

Next we define the singular integral and the singular series of the problem and record some related results.

Lemma 2.4. *Let $b_1, \dots, b_5$ be non-zero integers satisfying* (1.3)*. Also, let n be an integer and N be a natural number, and define*

$$\mathfrak{I}(n) = \frac{1}{32} \sum_{\substack{b_1 m_1 + \dots + b_5 m_5 = n \\ N/9 < |b_j| m_j \le N}} (m_1 \cdots m_5)^{-1/2}, \tag{2.11}$$

If either

(i) *$b_1, \dots, b_5$ are all positive, $n \ge 10 \max\{b_1, \dots, b_5\}$, and $N = n$; or*
(ii) *$b_1, \dots, b_5$ are not all of the same sign and $N \ge 10 \max\{|n|, |b_1|, \dots, |b_5|\}$,*

then

$$\mathfrak{I}(n) \asymp N^{3/2} |b_1 \cdots b_5|^{-1/2}. \tag{2.12}$$

Proof. This is essentially [1, Lemma 2.2]. □

If q is a positive integer, χ is a Dirichlet character mod q, and a is an integer, we define the exponential sums

$$C(\chi, a) = \sum_{1 \le h \le q} \bar{\chi}(h) e_q\left(ah^2\right) \qquad \text{and} \qquad C(q, a) = C(\chi_0, a),$$

where χ_0 is the principal character mod q; we also use the Gaussian sum

$$\tau(\chi, a) = \sum_{1 \le h \le q} \bar{\chi}(h) e_q(ah).$$

Furthermore, for any Dirichlet characters χ_j mod q_j $(j = 1, \dots, 5)$ and for any positive integer q such that $[q_1, \dots, q_5] \mid q$, we let χ_0 be the principal character mod q and write

$$B(q) = B(q; \chi_1, \dots, \chi_5) = \sum_{\substack{1 \le a \le q \\ (a,q) = 1}} e_q(-an) C(\chi_1 \chi_0, ab_1) \cdots C(\chi_5 \chi_0, ab_5),$$

$$\mathfrak{S}(\mathbf{b}, x) = \sum_{q \le x} \phi(q)^{-5} A(q), \qquad A(q) = B(q; \chi_0, \dots, \chi_0), \tag{2.13}$$

where in the definitions of $A(q)$ and $B(q)$ the dependence on $\mathbf{b} = (n, b_1, \dots, b_5)$ has been suppressed for brevity. In particular, $\mathfrak{S}(\mathbf{b}) = \mathfrak{S}(\mathbf{b}, \infty)$ is the singular series of the problem.

Lemma 2.5. *If $(b_1, \dots, b_5) = 1$, the function $B(q; \chi_1, \dots, \chi_5)$ has the following properties.*

(a) *$B(q; \chi_1, \dots, \chi_5)$ is multiplicative in q. That is, if $q = q_1 q_2$, $(q_1, q_2) = 1$, and $\chi_j = \chi_{j,1} \chi_{j,2}$ with $\chi_{j,i}$ a character* mod q_i*, then*

$$B(q; \chi_1, \dots, \chi_5) = B(q_1; \chi_{1,1}, \dots, \chi_{5,1}) B(q_2; \chi_{1,2}, \dots, \chi_{5,2}).$$

(b) *For $j = 1, \dots, 5$, let χ_j be a primitive character* mod p^{α_j}*, and suppose that $\alpha \geq \theta + \max\{\alpha_1, \dots, \alpha_5, \theta\}$, where $\theta = 2$ or $\theta = 1$ according as $p = 2$ or $p > 2$. Then $B(p^\alpha; \chi_1, \dots, \chi_5) = 0$.*

(c) *For $j = 1, \dots, 5$, let χ_j be a primitive character* mod 2^{α_j}*, and suppose that $\alpha = \max\{\alpha_1, \dots, \alpha_5\} \geq 2$. Then $B(2^\alpha; \chi_1, \dots, \chi_5) = 0$.*

(d) *For Dirichlet characters χ_j* mod q*, we have*

$$B(q; \chi_1, \dots, \chi_5) = \sum_{\xi_1^2 = \chi_1} \cdots \sum_{\xi_5^2 = \chi_5} \tau(\xi_1, b_1) \cdots \tau(\xi_5, b_5) \overline{\tau(\xi_1 \cdots \xi_5, n)}, \tag{2.14}$$

where $\sum_{\xi^2 = \chi}$ denotes summation over the characters ξ mod q *such that $\xi^2 = \chi$.*

(e) *For $j = 1, \dots, 5$, let χ_j be a primitive character* mod r_j*, let $r = [r_1, \dots, r_5]$, and suppose that $r = 2^\alpha r_0$, $2 \nmid r_0$. Then*

$$B(qr; \chi_1, \dots, \chi_5) = \begin{cases} A(q) B(r; \chi_1, \dots, \chi_5) & \text{if } \alpha = 0, (r, q) = 1, \\ A(q/2) B(2r; \chi_1, \dots, \chi_5) & \text{if } \alpha \geq 3, (r, q) = 2, \\ 0 & \text{otherwise.} \end{cases}$$

(f) *We have*

$$B(q; \chi_1, \dots, \chi_5) \ll 32^{\omega(q)} q^{7/2} \prod_{j=1}^{5} (b_j, q)^{1/2}.$$

Proof. (a) See [5, Lemma 3.2].

(b) See [5, Lemma 3.4(b)].

(c) For any character χ mod q, we have

$$\begin{aligned} C(\chi, a) &= \frac{1}{\phi(q)} \sum_{1 \leq m \leq q} e_q(am) \sum_{1 \leq h \leq q} \bar{\chi}(h) \sum_{\xi \bmod q} \xi^2(h) \bar{\xi}(m) \\ &= \frac{1}{\phi(q)} \sum_{\xi \bmod q} \tau(\xi, a) \sum_{1 \leq h \leq q} \bar{\chi}(h) \xi^2(h) = \sum_{\xi^2 = \chi} \tau(\xi, a). \end{aligned} \tag{2.15}$$

Suppose now that χ_j is primitive mod 2^α, $\alpha \geq 2$. Since the square of a character mod 2^α has conductor $\leq 2^{\alpha-1}$, there is no character ξ mod 2^α with $\xi^2 = \chi_j$ and the sum on the right side of (2.15) is empty.

We remark that by the same argument $B(p^\alpha; \chi_1, \dots, \chi_5) = 0$, if for some j we have $\chi_j(-1) = -1$. In particular, we have $B(2^\alpha; \chi_1, \dots, \chi_5) = 0$ if some character has conductor 4.

(d) If $(a, q) = 1$, we have $\tau(\chi, ab) = \chi(a)\tau(\chi, b)$, and (2.15) yields

$$C(\chi, ab) = \sum_{\xi^2 = \chi} \tau(\xi, ab) = \sum_{\xi^2 = \chi} \xi(a) \tau(\xi, b).$$

The desired conclusion follows by applying this identity to the sums $C(\chi_i, ab_i)$ appearing in $B(q; \chi_1, \dots, \chi_5)$ and then interchanging the order of summation.

(e) This follows from parts (a)–(c) and the above remark about characters of conductor 4.

(f) This follows from [5, Lemma 3.1(c)] and part (a). Alternatively, one can deduce the result by combining (2.14) and known estimates for the Gaussian sum (see [6, Lemmas 5.1 and 5.4]). Moreover, the latter approach yields a sharper bound, in which the factor $q^{7/2}$ is replaced by $q^3 (n, q)^{1/2}$. □

Lemma 2.6. *Let $n, b_1, \dots, b_5$ be integers satisfying* (1.2) *and* (1.3)*, and suppose that at most two among them are divisible by* 5*. Let $\mathfrak{S}(\mathbf{b}, x)$ be defined by* (2.13)*. Then the infinite series $\mathfrak{S}(\mathbf{b}) = \mathfrak{S}(\mathbf{b}, \infty)$ is absolutely convergent and satisfies*

$$\mathfrak{S}(\mathbf{b}) \gg (\log\log B)^{-c}, \tag{2.16}$$

where $B = \max\{10, |b_1|, \dots, |b_5|\}$. Furthermore, for any fixed $\varepsilon > 0$, we have

$$|\mathfrak{S}(\mathbf{b}) - \mathfrak{S}(\mathbf{b}, x)| \ll x^{-1+\varepsilon} B^{\varepsilon}. \tag{2.17}$$

Proof. These are established in [1, Lemma 7.1]. We remark that references in that proof to [1, eq. (1.3)] can be replaced by references to (1.3) above. □

Lemma 2.7. *For $j = 1, \dots, 5$, let χ_j be a primitive character* mod r_j*, let $r = [r_1, \dots, r_5]$, and suppose that $b_1, \dots, b_5$ satisfy* (1.3)*. Then, for any fixed $\varepsilon > 0$,*

$$\sum_{q \le x/r} \phi(qr)^{-5} B(qr; \chi_1, \dots, \chi_5) \ll r^{-1/2+\varepsilon} (\log(x+2))^5. \tag{2.18}$$

Proof. Let $r' = r$ or $2r$ according as $8 \nmid r$ or $8 \mid r$. By Lemma 2.5(e), the left side of (2.18) is

$$\phi(r')^{-5} B(r'; \chi_1, \dots, \chi_5) \sum_{\substack{q \le x/r' \\ (q,r)=1}} \phi(q)^{-5} A(q). \tag{2.19}$$

In order to bound the sum over q, we need an estimate for $A(q)$ that takes into account the extra cancelation that occurs on the right side of (2.14) when all the characters are principal. We first record the inequality $|A(p)| \le 4p^4$, which can be derived from [5, eq. (3.10)] via case-by-case analysis. By parts (a)–(c) of Lemma 2.5, we then have

$$A(q) \ll \prod_{p \mid q} |A(p)| \ll 4^{\omega(q)} q^4. \tag{2.20}$$

Using Lemma 2.5(f) to bound $B(r')$ and (2.20) to bound the sum over q, we find that (2.19) is bounded above by

$$33^{\omega(r)} r^{-3/2} \prod_{j=1}^{5} (b_j, r)^{1/2} \sum_{q \le x/r} 5^{\omega(q)} q^{-1}.$$

Hence, the desired result follows from (1.3). □

3. Proof of the theorem

Let N be a parameter with

$$N \ge |b_5| |b_1 \cdots b_4|^{4+\varepsilon} \tag{3.1}$$

that also satisfies hypothesis (i) or (ii) of Lemma 2.4 according as $b_1, \dots, b_5$ are all positive or not. Throughout the proof, we set $\eta = \varepsilon/1000$ and write

$$L = \log N, \quad N_j = (N/|b_j|)^{1/2}, \quad \text{and} \quad X = N_1 \cdots N_5 N^{-1}.$$

We will use the circle method to show that the quantity

$$r(n) = \sum_{\substack{n = b_1 p_1^2 + \cdots + b_5 p_5^2 \\ N/9 < |b_j| p_j^2 \le N}} (\log p_1) \cdots (\log p_5)$$

is positive. Clearly, this establishes Theorem 1.

We need to introduce some notation. Define the exponential sums

$$S_j(\alpha) = \sum_{N_j/3<p\le N_j} (\log p) e\left(\alpha b_j p^2\right) \qquad (1 \le j \le 5),$$

and for any measurable set $\mathfrak{B} \subseteq [0,1]$ write

$$r(n,\mathfrak{B}) = \int_{\mathfrak{B}} S_1(\alpha)\cdots S_5(\alpha) e(-n\alpha)\, d\alpha. \tag{3.2}$$

In particular, by orthogonality, we have $r(n) = r(n,[0,1])$. Let P be a parameter to be chosen later. The primary Hardy–Littlewood decomposition of the unit interval into sets of major and minor arcs is given by

$$\mathfrak{M} = \bigcup_{q\le P} \bigcup_{\substack{0\le a\le q\\(a,q)=1}} \mathfrak{M}(q,a;P) \qquad \text{and} \qquad \mathfrak{m} = [0,1]\setminus \mathfrak{M}, \tag{3.3}$$

where if $1 \le Q \le N$, we define the major arc $\mathfrak{M}(q,a;Q)$ by

$$\mathfrak{M}(q,a;Q) = \left\{\alpha \in [0,1] : |q\alpha - a| < QN^{-1}\right\}.$$

We also use a secondary decomposition of the set of major arcs $\mathfrak{M}$. Let $R = N^{6\eta}$. We define the sets

$$\mathfrak{M}_0 = \bigcup_{q\le R} \bigcup_{\substack{0\le a\le q\\(a,q)=1}} \mathfrak{M}(q,a;R), \qquad \mathfrak{N} = \mathfrak{M}\setminus \mathfrak{M}_0, \tag{3.4}$$

and

$$\mathfrak{N}(q) = \begin{cases} \mathfrak{M}(q,0;P)\setminus \mathfrak{M}(q,0;R) & \text{if } 1 \le q \le R,\\ \mathfrak{M}(q,0;P) & \text{if } R < q \le P.\end{cases}$$

Let us consider $r(n,\mathfrak{M})$. We are going to combine the approaches used to deal with the major arcs in [1] and in [4]. First, we employ the method in [1] to estimate $r(n,\mathfrak{M}_0)$. Using Lemma 2.7 above in the place of [1, Lemma 3.1], we can proceed as in the proof of [1, Theorem 3] to obtain

$$r(n,\mathfrak{M}_0) = \mathfrak{S}(\mathbf{b},R)\mathfrak{I}(n) + O\big(XL^{-1}\big), \tag{3.5}$$

with $\mathfrak{I}(n)$ and $\mathfrak{S}(\mathbf{b},x)$ given by (2.11) and (2.13) above. Since Lemma 2.7 features the term $r^{-1/2+\varepsilon}$ in place of the term $r^{-1+\varepsilon}$ appearing in [1, Lemma 3.1], we need to replace the terms $r^{-1/5+\varepsilon}$ in the definitions of J_j and K_j in [1] by $r^{-1/10+\varepsilon}$. However, this change does not affect the proofs of Lemmas 4.1 and 5.1 in [1] when the parameter P in [1] is chosen equal to $R = N^{6\eta}$.

Next, we use the approach in [4] to bound $r(n,\mathfrak{N})$. When $\alpha \in \mathfrak{M}(q,a;P)$, (2.5) yields

$$S_j(\alpha) \ll N_j^{11/20+\eta}(q(1+N|\beta|))^{1/2} + \frac{(q,b_j)^{1/2}N_j^{1+\eta}}{(q(1+N|\beta|))^{1/2}} \quad (1 \le j \le 5),$$

with $\beta = \alpha - a/q \in \mathfrak{N}(q)$. Recalling (1.3), we deduce that

$$r(n,\mathfrak{N}) \le \sum_{q\le P} \sum_{\substack{1\le a\le q\\(a,q)=1}} \int_{\mathfrak{N}(q)} \left|S_1\left(\frac{a}{q}+\beta\right)\cdots S_5\left(\frac{a}{q}+\beta\right)\right| d\beta \tag{3.6}$$
$$\ll \sum_{k=0}^{5} \frac{(NX)^{1+\eta}}{(N_1\cdots N_k)^{9/20}} \sum\nolimits_k{}',$$

where for $k = 0, 1, \dots, 5$,

$$\begin{aligned}\sum\nolimits_k &= \sum_{q\le P} (q, b_1\cdots b_5) q^{k-3/2} \int_{\mathfrak{N}(q)} \frac{d\beta}{(1+N|\beta|)^{5/2-k}}\\ &\ll N^{-1} \sum_{q\le P} (q, b_1\cdots b_5) \left(P^{k-3/2} + (R+q)^{k-3/2}\right)\\ &\ll |b_1|^{\eta} N^{-1} \left(P^{k-1/2} + R^{k-1/2}\right).\end{aligned}$$

Substituting this bound into the right side of (3.6), we obtain

$$r(n,\mathfrak{N}) \ll X^{1+2\eta}\left\{R^{-1/2} + \sum_{k=1}^{5} P^{k-1/2}(N_1\cdots N_k)^{-9/20}\right\}.$$

Hence,

$$r(n,\mathfrak{N}) \ll XN^{-\eta}, \tag{3.7}$$

provided that

$$P \le \min_{1\le k\le 5} (N_1\cdots N_k)^{9/(10(2k-1))-6\eta}. \tag{3.8}$$

We now turn to the estimation of $r(n,\mathfrak{m})$. When $\alpha \in \mathfrak{m}$, there exist integers a and q satisfying (2.7) with $b = b_5$ and $X = N_5$ and such that $q + N|q\alpha - a| \ge P$. Thus, if P satisfies

$$2|b_5| N_5^{1/4} \le P \le N_5, \tag{3.9}$$

we can apply Lemma 2.3 to get

$$\sup_{\alpha\in\mathfrak{m}} |S_5(\alpha)| \ll N_5^{7/8+\eta} + N^{1/2+\eta}P^{-1/2} \ll N_5^{7/8+3\eta}.$$

Combining this bound with the inequality (see [1, eq. (2.9)])

$$\int_0^1 |S_1(\alpha)\cdots S_4(\alpha)|\, d\alpha \ll (N_1\cdots N_4)^{1/2+\eta},$$

we obtain

$$\begin{aligned}r(n,\mathfrak{m}) &\le \Big(\sup_{\alpha\in\mathfrak{m}} |S_5(\alpha)|\Big) \int_0^1 |S_1(\alpha)\cdots S_4(\alpha)|\, d\alpha\\ &\ll N_5^{7/8+3\eta}(N_1\cdots N_4)^{1/2+\eta} \ll XN^{-\eta},\end{aligned} \tag{3.10}$$

in view of (3.1).

Finally, we are in position to complete the proof. We set

$$P = (N_1\cdots N_5)^{1/10-6\eta}.$$

When (3.1) holds, this choice of P satisfies (3.8) and (3.9), and we conclude from (2.12), (2.16), (2.17), (3.2)–(3.5), (3.7), and (3.10) that

$$r(n) = \mathfrak{S}(\mathbf{b}, R)\mathfrak{J}(n) + O\left(XL^{-1}\right) \gg X(\log L)^{-c},$$

which suffices to complete the proof. □

References

[1] S. K. K. Choi and J. Y. Liu, *Small prime solutions of quadratic equations*, Canad. J. Math. **54** (2002), 71-91.

[2] ———, *Small prime solutions of quadratic equations II*, to appear.

[3] A. V. Kumchev, *On Weyl sums over primes and almost primes*, to appear.

[4] ———, *On the Waring-Goldbach problem: Exceptional sets for sums of cubes and higher powers*, to appear.

[5] M. C. Liu and K. M. Tsang, *Small prime solutions of some additive equations*, Monatsh. Math. **111** (1991), 147–169.

[6] H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

Department of Mathematics and Statistics, Simon Fraser University, Burnaby, British Columbia, Canada V5A 1S6

E-mail address: kkchoi@math.sfu.ca

Department of Mathematics, 1 University Station C1200, The University of Texas at Austin, Austin, TX 78712, U.S.A.

E-mail address: kumchev@math.utexas.edu