Diophantine Methods for Exponential Sums, and Exponential Sums for Diophantine Problems

Trevor D. Wooley*

Abstract

Recent developments in the theory and application of the Hardy-Littlewood method are discussed, concentrating on aspects associated with diagonal diophantine problems. Recent efficient differencing methods for estimating mean values of exponential sums are described first, concentrating on developments involving smooth Weyl sums. Next, arithmetic variants of classical inequalities of Bessel and Cauchy-Schwarz are discussed. Finally, some emerging connections between the circle method and arithmetic geometry are mentioned.

2000 Mathematics Subject Classification: 11P55, 11L07, 11P05, 11D72, 14G05.
Keywords and Phrases: The Hardy-Littlewood method, exponential sums, Waring's problem, equations in many variables, rational points, representation problems.

1. Introduction

Over the past fifteen years or so, the Hardy-Littlewood method has experienced a renaissance that has left virtually no facet untouched in its application to diophantine problems. Our purpose in this paper is to sketch what might be termed the past, present, and future of these developments, concentrating on aspects associated with diagonal diophantine problems, and stressing modern developments that make increasing use of less traditional diophantine input within ambient analytic methods. We avoid discussion of the Kloosterman method and its important recent variants (see [5] and [8]), because the underlying ideas seem inherently constrained to quadratic, and occasionally cubic, diophantine problems. Our account begins with a brief introduction to the Hardy-Littlewood (circle) method, using Waring's problem as the basic example. The discussion here illustrates well the issues involved in the analysis of systems of diagonal equations over arbitrary algebraic extensions of $\mathbb{Q}$, and motivates that associated with more general systems of homogeneous equations (see [1] and [14]).

*Department of Mathematics, University of Michigan, East Hall, 525 East University Avenue, Ann Arbor, Michigan 48109-1109, USA. E-mail: wooley@umich.edu

Let s and k be natural numbers with $s > k \geq 2$, and consider an integer n sufficiently large in terms of s and k. The circle method employs Fourier analysis in order to obtain asymptotic information concerning the number, $R(n) = R_{s,k}(n)$, of integral solutions of the equation $x_1^k + \cdots + x_s^k = n$. Write $P = n^{1/k}$ and define the exponential sum $f(\alpha) = f(\alpha; P)$ by

$$f(\alpha) = \sum_{1 \leq x \leq P} e(\alpha x^k),$$

wherein $e(z)$ denotes $e^{2\pi i z}$. Then it follows from orthogonality that

$$R(n) = \int_0^1 f(\alpha)^s e(-n\alpha) d\alpha.$$

When α is well-approximated by rational numbers with small denominators, one has sharp asymptotic information concerning $f(\alpha)$. In order to be precise, let Q satisfy $1 \leq Q \leq \frac{1}{2}P^{k/2}$, and define the *major arcs* $\mathfrak{M} = \mathfrak{M}(Q)$ to be the union of the intervals $\mathfrak{M}(q, a) = \{\alpha \in [0, 1) : |q\alpha - a| \leq QP^{-k}\}$, with $0 \leq a \leq q \leq Q$ and $(a, q) = 1$. Also, put

$$S(q, a) = \sum_{r=1}^{q} e(ar^k/q) \quad \text{and} \quad v(\beta) = \int_0^P e(\beta\gamma^k) d\gamma,$$

and define $f^*(\alpha)$ for $\alpha \in [0, 1)$ by taking $f^*(\alpha) = q^{-1}S(q, a)v(\alpha - a/q)$, when α lies in $\mathfrak{M}(q, a) \subseteq \mathfrak{M}(Q)$, and otherwise by setting $f^*(\alpha) = 0$. Then the sharpest available estimate (see Theorem 4.1 of [16]) establishes that[1] $f(\alpha) = f^*(\alpha) + O(Q^{1/2+\epsilon})$, uniformly for $\alpha \in \mathfrak{M}(Q)$. The functions $S(q, a)$ and $v(\beta)$ are rather well-understood, and thus one deduces that whenever $s \geq \max\{4, k + 1\}$ and $Q \leq P$, then

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha) d\alpha = \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} \mathfrak{S}_{s,k}(n) n^{s/k-1} + O(n^{s/k-1-\delta}), \tag{1.1}$$

for a suitable positive number δ. Here, the Γ-function is that familiar from classical analysis, and the *singular series* $\mathfrak{S}_{s,k}(n)$ is equal to the product of p-adic densities $\prod_p v_p(n)$, where for each prime p we write

$$v_p(n) = \lim_{h \to \infty} p^{h(1-s)} \text{card}\{\mathbf{x} \in (\mathbb{Z}/p^h\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv n \pmod{p^h}\}.$$

An asymptotic formula for $R(n)$, with leading term determined by the major arc contribution (1.1), now follows provided that the corresponding contribution

[1] Given a complex-valued function $f(t)$ and positive function $g(t)$, we use Vinogradov's notation $f(t) \ll g(t)$, or Landau's notation $f(t) = O(g(t))$, to mean that when t is large, there is a positive number C for which $f(t) \leq Cg(t)$. Similarly, we write $f(t) \gg g(t)$ when $g(t) \ll f(t)$, and $f(t) \asymp g(t)$ when $f(t) \ll g(t) \ll f(t)$. Also, we write $f(t) = o(g(t))$ when as $t \to \infty$, one has $f(t)/g(t) \to 0$. Finally, we use the convention that whenever ϵ occurs in a formula, then it is asserted that the statement holds for each fixed positive number ϵ.

arising from the minor arcs $\mathfrak{m} = [0,1) \setminus \mathfrak{M}$ is asymptotically smaller. Although such is conjectured to hold as soon as $s \geq \max\{4, k+1\}$, this is currently known only for larger values of s. It is here that energy is focused in current research. One typically estimates the minor arc contribution via an inequality of the type

$$\left|\int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha)d\alpha\right| \leq \left(\sup_{\alpha\in\mathfrak{m}} |f(\alpha)|\right)^{s-2t} \int_0^1 |f(\alpha)|^{2t} d\alpha. \tag{1.2}$$

For suitable choices of t and Q, one now seeks bounds of the shape

$$\sup_{\alpha\in\mathfrak{m}} |f(\alpha)| \ll P^{1-\tau+\epsilon} \quad \text{and} \quad \int_0^1 |f(\alpha)|^{2t} d\alpha \ll P^{2t-k+\delta+\epsilon}, \tag{1.3}$$

with $\tau > 0$ and δ small enough that $(s-2t)\tau > \delta$. The right hand side of (1.2) is then $o(n^{s/k-1})$, which is smaller than the main term of (1.1) whenever $\mathfrak{S}_{s,k}(n) \gg 1$. The latter is assured provided that non-singular p-adic solutions can be found for each prime p, and in any case when $s \geq 4k$. Classically, one has two apparently incompatible approaches toward establishing the estimates (1.3). On one side is the differencing approach introduced by Weyl [23], and pursued by Hua [9], that yields an asymptotic formula for $R(n)$ whenever $s \geq 2^k + 1$. The ideas introduced by Vinogradov [21], meanwhile, provide the desired asymptotic formula when $s > Ck^2 \log k$, for a suitable positive constant C.

2. Efficient differencing and smooth Weyl sums

Since the seminal work of Vaughan [15], progress on diagonal diophantine problems has been based, almost exclusively, on the use of smooth numbers, by which we mean integers free of large prime factors. In brief, one seeks serviceable substitutes for the estimates (1.3) with the underlying summands restricted to be smooth, the hope being that this restriction might lead to sharper bounds. Before describing the kind of conclusions now available, we must introduce some notation. Let $\mathcal{A}(P,R)$ denote the set of natural numbers not exceeding P, all of whose prime divisors are at most R, and define the associated exponential sum $h(\alpha) = h(\alpha; P, R)$ by

$$h(\alpha; P, R) = \sum_{x\in\mathcal{A}(P,R)} e(\alpha x^k).$$

When t is a positive integer, we consider the mean value $S_t(P,R) = \int_0^1 |h(\alpha)|^{2t} d\alpha$, which, by orthogonality, is equal to the number of solutions of the diophantine equation $x_1^k + \cdots + x_t^k = y_1^k + \cdots + y_t^k$, with $x_i, y_i \in \mathcal{A}(P,R)$ $(1 \leq i \leq t)$. We take $R \asymp P^\eta$ in the ensuing discussion, with η a small positive number[2]. In these circumstances one has $\text{card}(\mathcal{A}(P,R)) \sim c(\eta)P$, where the positive number $c(\eta)$ is

[2] We adopt the convention that whenever η appears in a statement, implicitly or explicitly, then it is asserted that the statement holds whenever $\eta > 0$ is sufficiently small in terms of ϵ.

given by the Dickman function, and it follows that $S_t(P,R) \gg P^t + P^{2t-k}$. It is conjectured that in fact $S_t(P,R) \ll P^\epsilon(P^t + P^{2t-k})$. We refer to the exponent λ_t as being *permissible* when, for each $\epsilon > 0$, there exists a positive number $\eta = \eta(t,k,\epsilon)$ with the property that whenever $R \le P^\eta$, one has $S_t(P,R) \ll P^{\lambda_t+\epsilon}$. One expects that the exponent $\lambda_t = \max\{t, 2t-k\}$ should be permissible, and with this in mind we say that δ_t is an *associated exponent* when $\lambda_t = t + \delta_t$ is permissible, and that Δ_t is an *admissible exponent* when $\lambda_t = 2t - k + \Delta_t$ is permissible.

The computations required to determine sharp permissible exponents for a specific value of k are substantial (see [20]), but for larger k one may summarise some general features of these exponents. First, for $0 \le t \le 2$ and $k \ge 2$, it is essentially classical that the exponent $\delta_t = 0$ is associated, and recent work of Heath-Brown [6] provides the same conclusion also when $t = 3$ and $k \ge 238{,}607{,}918$. When $t = o(\sqrt{k})$, one finds that associated exponents exhibit *quasi-diagonal behaviour*, and satisfy the property that $\delta_t \to 0$ as $k \to \infty$. To be precise, Theorem 1.3 of [28] shows that whenever $k \ge 3$ and $2 < t \le 2e^{-1}k^{1/2}$, then the exponent

$$\delta_t = \frac{4k^{1/2}}{et} \exp\left(-\frac{4k}{e^2t^2}\right), \tag{2.1}$$

is associated. For larger t, methods based on repeated efficient differencing yield the sharpest estimates. Thus, the corollary to Theorem 2.1 of [26] establishes that for $k \ge 4$, an admissible exponent Δ_t is given by the positive solution of the equation $\Delta_t e^{\Delta_t/k} = ke^{1-2t/k}$. The exponent $\lambda_t = 2t - k + ke^{1-2t/k}$ is therefore always permissible. Previous to repeated efficient differencing, analogues of these permissible exponents had a term of size $ke^{-t/k}$ in place of $ke^{1-2t/k}$ (see [15]), so that in a sense, the modern theory is twice as powerful as that available hitherto.

The above discussion provides a useable analogue of the mean-value estimate in (1.3). We turn next to localised minor arc estimates. Take $Q = P$, and define $\mathfrak{m}$ as in the introduction. Suppose that s, t and w are parameters with $2s \ge k+1$ for which Δ_s, Δ_t and Δ_w are admissible exponents, and define

$$\sigma(k) = \frac{k - \Delta_t - \Delta_s\Delta_w}{2(s(k + \Delta_w - \Delta_t) + tw(1 + \Delta_s))}.$$

Then Corollary 1 to Theorem 4.2 of [27] shows that $\sup_{\alpha\in\mathfrak{m}} |h(\alpha)| \ll P^{1-\sigma(k)+\epsilon}$, and for large k this estimate holds with $\sigma(k)^{-1} = k(\log k + O(\log\log k))$. Applying an analogue of (1.2) with h in place of f, and taking[3] $t = [\frac{1}{2}k(\log k + \log\log k + 1)]$ and $s = 2t + k + [Ak\log\log k/\log k]$, for a suitable $A > 0$, we deduce from our discussion of permissible exponents that $\int_{\mathfrak{m}} h(\alpha)^s e(-n\alpha)d\alpha = o(n^{s/k-1})$. By considering the representations of a given integer n with all of the kth powers R-smooth, it is now apparent that a modification of the argument sketched in the introduction shows that $R(n) \gg \mathfrak{S}_{s,k}(n)n^{s/k-1}$ as soon as one confirms that

$$\int_{\mathfrak{M}} h(\alpha)^s e(-n\alpha)d\alpha \sim c(\eta)^s \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} \mathfrak{S}_{s,k}(n)n^{s/k-1}. \tag{2.2}$$

[3]We write $[z]$ to denote $\max\{n \in \mathbb{Z} : n \le z\}$.

Sharp asymptotic information concerning $h(\alpha)$ is available throughout $\mathfrak{M}(Q)$ only when Q is a small power of $\log P$, and so the proof of (2.2) involves pruning technology. Such machinery, in this case designed to estimate the contribution from a set of the shape $\mathfrak{M}(P)\setminus\mathfrak{M}((\log P)^\delta)$, has evolved into a powerful tool. Such issues can be handled these days with a number of variables barely exceeding $\max\{4,k+1\}$.

This approach leads to the best known upper bounds on the function $G(k)$ in Waring's problem, defined to be the least integer r for which all sufficiently large natural numbers are the sum of at most r positive integral kth powers.

Theorem 2.1. *One has* $G(k)\le k(\log k+\log\log k+2+O(\log\log k/\log k))$.

This upper bound (Theorem 1.4 of [27]) refines an earlier one of asymptotically similar strength (Corollary 1.2.1 of [24]) that gave the first sizeable improvement of Vinogradov's celebrated bound $G(k)\le(2+o(1))k\log k$, dating from 1959 (see [22]). Aside from Linnik's bound $G(3)\le 7$ (see [11]), all of the sharpest known bounds on $G(k)$ for smaller k are established using variants of these methods. Thus one has $G^{\#}(4)\le 12$ (see [15], and here the # denotes that there are congruence conditions modulo 16), $G(5)\le 17$, $G(6)\le 24$, $G(7)\le 33$, $G(8)\le 42$, $G(9)\le 50$, $G(10)\le 59$, $G(11)\le 67$, $G(12)\le 76$, $G(13)\le 84$, $G(14)\le 92$, $G(15)\le 100$, $G(16)\le 109$, $G(17)\le 117$, $G(18)\le 125$, $G(19)\le 134$, $G(20)\le 142$ (see [17], [18], [19], [20]).

Unfortunately, shortage of space obstructs any but the crudest account of the ideas underlying the proof of the mean value estimates that supply the above permissible exponents. The use of exponential sums over smooth numbers occurs already in work of Linnik and Karatsuba (see [10]), but only with Vaughan's new iterative method [15] is a flexible homogeneous approach established. An alternative formulation suitable for repeated efficient differencing is introduced by the author in [24]. Suppose that the exponent λ_s is permissible, and consider a polynomial $\psi\in\mathbb{Z}[t]$ of degree $d\ge 2$. Given positive numbers M and T with $M\le T$, and an element $x\in\mathcal{A}(T,R)$ with $x>M$, there exists an integer m with $m\in[M,MR]$ for which $m|x$. Consequently, by applying a *fundamental lemma* of combinatorial flavour, one may bound the number of integral solutions of the equation

$$\psi(z)-\psi(w)=\sum_{i=1}^{s}(x_i^k-y_i^k), \tag{2.3}$$

with $1\le z,w\le P$ and $x_i,y_i\in\mathcal{A}(T,R)$ $(1\le i\le s)$, in terms of the number of integral solutions of the equation

$$\psi(z)-\psi(w)=m^k\sum_{i=1}^{s}(u_i^k-v_i^k), \tag{2.4}$$

with $1\le z,w\le P$, $M<m\le MR$, $(\psi'(z)\psi'(w),m)=1$ and $u_i,v_i\in\mathcal{A}(T/M,R)$ $(1\le i\le s)$. The implicit congruence condition $\psi(z)\equiv\psi(w)\pmod{m^k}$ may be analytically refined to the stronger one $z\equiv w\pmod{m^k}$, and in this way one is led to replace the expression $\psi(z)-\psi(w)$ by the difference polynomial

$\psi_1(z;h;m) = m^{-k}(\psi(z+hm^k) - \psi(z))$. Notice that when $M \geq P^{1/k}$, one is forced to conclude that $z = w$, and then the number of solutions of (2.4) is bounded above by $PMRS_s(T/M,R) \ll P^{1+\epsilon}M(T/M)^{\lambda_s}$. Otherwise, following an application of Schwarz's inequality to the associated mean value of exponential sums, one may recover an equation of the shape (2.3) in which $\psi(z)$ is replaced by $\psi_1(z)$, and T is replaced by T/M, and repeat the process once again. This gives a repeated differencing process that hybridises that of Weyl with the ideas of Vinogradov.

It is now possible to describe a strategy for bounding a permissible exponent λ_{s+1} in terms of a known permissible exponent λ_s. We initially take $T = P$ and $\psi(z) = z^k$, and observe that $S_{s+1}(P,R)$ is bounded above by the number of solutions of (2.3). We apply the above efficient differencing process successively with appropriate choices for M at each stage, say $M = P^{\phi_i}$, with $0 \leq \phi_i \leq 1/k$, for the ith differencing operation. After some number of steps, say j, we take $\phi_j = 1/k$ in order to force the above diagonal situation that is easily estimated. One then optimises choices for the ϕ_i in order to extract the sharpest upper bound for $S_{s+1}(P,R)$, and this in turn yields a permissible exponent λ_{s+1}. It transpires that in this simplified treatment, successive admissible exponents are related by the formula $\Delta_{s+1} = \Delta_s(1-\phi) + k\phi - 1$, wherein one may take ϕ very close to $1/(k+\Delta_s)$. Thus one finds that Δ_{s+1} is essentially $\Delta_s(1-2/(k+\Delta_s))$, an observation that goes some way to explaining how it is that this method is about twice as strong as previous approaches that would correspond to choices of ϕ close to $1/k$.

Refined versions of this differencing process make use of all known permissible exponents λ_s in order to estimate a particular exponent λ_t, and in such circumstances the process becomes highly iterative, and entails significant computation. Such variants make use of refined Weyl estimates for difference polynomials, and estimates for the number of integral points on curves and surfaces (see [20]). Variants of these methods apply also in the situation of Vinogradov's mean value theorem (see [25]), smooth Weyl sums with polynomial arguments (see [29]), and even for sums relevant to counting rational lines on hypersurfaces (see [12]).

Frequent reference to underlying diophantine equations seems to limit these methods to estimating even moments of smooth Weyl sums, and until recently fractional moments could be estimated only by applying Hölder's inequality to interpolate linearly between permissible exponents. However, a method [28] is now available that permits fractional moments to be estimated non-trivially, thereby "breaking classical convexity", and moreover the number of variables being differenced need not even be an integer. These new estimates can be applied to sharpen permissible exponents (with integral argument), and indeed the associated exponent (2.1) is established in this way. Another consequence [32] of these developments is the best available lower bound for $N(X)$, which we define to be the number of integers not exceeding X that are represented as the sum of three positive integral cubes. One has $N(X) \gg X^{1-\xi/3-\epsilon}$, where $\xi = (\sqrt{2833}-43)/41 = 0.24941301\ldots$ arises from the permissible exponent $\lambda_3 = 3+\xi$ for $k=3$. Earlier, Vaughan [15] obtained an estimate of the latter type with $13/4$ in place of $3+\xi$.

3. Arithmetic variants of Bessel's inequality

Already in our opening paragraph we alluded to some of the applications accessible to the methods of §2. We now turn to less obvious applications that have experienced recent progress. We illustrate ideas once again with a simple example, and consider the set $\mathcal{Z}(N)$ of integers n, with $N/2 < n \le N$, that are *not* represented as the sum of s positive integral kth powers. The standard approach to estimating $Z(N) = \text{card}(\mathcal{Z}(N))$ is via Bessel's inequality. We now take $P = N^{1/k}$. When $\mathfrak{B} \subseteq [0,1)$, write $R^*(n;\mathfrak{B}) = \int_{\mathfrak{B}} h(\alpha)^s e(-n\alpha)d\alpha$, and write also $R^*(n) = R^*(n;[0,1))$. The theory of §2 ensures that when Q is a sufficiently small power of $\log P$, and $s \ge 4k$, then $R^*(n;\mathfrak{M}) \asymp n^{s/k-1}$. Under such circumstances, an application of Bessel's inequality reveals that $Z(N)$ is bounded above by

$$\sum_{N/2<n\le N} \left| \frac{R^*(n) - R^*(n;\mathfrak{M})}{R^*(n;\mathfrak{M})} \right|^2 \ll (N^{s/k-1})^{-2} \sum_{n\in\mathbb{N}} \left| \int_{\mathfrak{m}} h(\alpha)^s e(-n\alpha)d\alpha \right|^2$$
$$\ll (N^{s/k-1})^{-2} \int_{\mathfrak{m}} |h(\alpha)|^{2s} d\alpha. \tag{3.1}$$

When $s \ge \frac{1}{2}k(\log k + \log\log k + 2 + o(1))$, the minor arc integral in (3.1) is $o(N^{2s/k-1})$, and thus it follows that $Z(N) = o(N)$. Thus one may conclude that almost all integers are sums of $s \sim (\frac{1}{2} + o(1))k\log k$ positive integral kth powers.

The application of Bessel's inequality in (3.1) makes inefficient use of underlying arithmetic information, and fails, for example, to effectively estimate the number of values of a polynomial sequence not represented in some prescribed form. Suppose instead that we define a Fourier series over the exceptional set itself, namely $K(\alpha) = \sum_n e(n\alpha)$, where the summation is over $n \in \mathcal{Z}(N)$. Since $R^*(n) = 0$ for $n \in \mathcal{Z}(N)$, one has $R^*(n;\mathfrak{m}) = -R^*(n;\mathfrak{M})$, and thus we see that

$$N^{s/k-1} Z(N) \ll \int_{\mathfrak{M}} h(\alpha)^s K(-\alpha)d\alpha = \left| \int_{\mathfrak{m}} h(\alpha)^s K(-\alpha)d\alpha \right|.$$

Applying Schwarz's inequality in combination with Parseval's identity, we recover the previous consequence of Bessel's inequality via the bound

$$\left| \int_{\mathfrak{m}} h(\alpha)^s K(-\alpha)d\alpha \right| \le \left(\int_0^1 |K(\alpha)|^2 d\alpha \right)^{1/2} \left(\int_{\mathfrak{m}} |h(\alpha)|^{2s} d\alpha \right)^{1/2}. \tag{3.2}$$

However, this formulation permits alternate applications of Schwarz's inequality or Hölder's inequality. For example, the left hand side of (3.2) is bounded above by

$$\left(\int_0^1 |h(\alpha)^{2t} K(\alpha)^2| d\alpha \right)^{1/2} \left(\int_{\mathfrak{m}} |h(\alpha)|^{2s-2t} d\alpha \right)^{1/2}, \tag{3.3}$$

and also by

$$\left(\int_0^1 |K(\alpha)|^4 d\alpha \right)^{1/4} \left(\int_{\mathfrak{m}} |h(\alpha)|^{4s/3} d\alpha \right)^{3/4}. \tag{3.4}$$

In either case, the diophantine equations underlying the integrals on the left hand sides of (3.3) and (3.4) contain arithmetic information that can be effectively exploited whenever the set $\mathcal{Z}(N)$ is reasonably thin.

The strategy sketched above has been exploited by Brüdern, Kawada and Wooley in a series of papers devoted to additive representation of polynomial sequences. Typical of the kind of results now available is the conclusion [3] that almost all values of a given integral cubic polynomial are the sum of six positive integral cubes. Also, Wooley [30], [31], has derived improved (slim) exceptional set estimates in Waring's problem when excess variables are available. For example, write $E(N)$ for the number of integers n, with $1 \le n \le N$, for which the anticipated asymptotic formula *fails* to hold for the number of representations of an integer as the sum of a square and five cubes of natural numbers. Then in [31] it is shown that $E(N) \ll N^{\epsilon}$.

As a final illustration of such ideas, we highlight an application to the solubility of pairs of diagonal cubic equations. Fix $k = 3$, define $h(\alpha)$ as in §2, and put $c(n) = \int_0^1 |h(\alpha)|^5 e(-n\alpha) d\alpha$ for each $n \in \mathbb{N}$. Brüdern and Wooley [4] have applied the ideas sketched above to estimate the frequency with which large values of $|c(n)|$ occur, and thereby have shown that, with ξ defined as in the previous section,

$$\sum_{x,y \in \mathcal{A}(P,R)} |c(x^3 - y^3)|^2 = \int_0^1 \int_0^1 |h(\alpha)^5 h(\beta)^5 h(\alpha+\beta)^2| d\alpha d\beta \ll P^{6+\xi+\epsilon}.$$

On noting that $6 + \xi < 6.25$, cognoscenti will recognise that this twelfth moment of smooth Weyl sums, in combination with a classical exponential sum equipped with Weyl's inequality, permits the discussion of pairs of diagonal cubic equations in 13 variables via the circle method. The exponent $6 + \xi$ improves an exponent $6 + 2\xi$ previously available for a (different) twelfth moment. Brüdern and Wooley [4] establish the following conclusion.

Theorem 3.1. *Suppose that $s \ge 13$, and that a_i, b_i $(1 \le i \le s)$ are fixed integers. Then the Hasse principle holds for the pair of equations*

$$a_1 x_1^3 + \cdots + a_s x_s^3 = b_1 x_1^3 + \cdots + b_s x_s^3 = 0.$$

The condition $s \ge 13$ improves on the previous bound $s \ge 14$ due to Brüdern [2], and achieves the theoretical limit of the circle method for this problem.

4. Arithmetic geometry via descent

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a homogeneous polynomial of degree d, and consider the number, $N(B)$, of integral zeros of the equation $F(\mathbf{x}) = 0$, with $\mathbf{x} \in [-B, B]^s$. When s is sufficiently large in terms of d, the circle method shows under modest geometric conditions that $N(B)$ is asymptotic to the expected product of local densities. For fairly general polynomials, the condition on s is as severe as $s > (d-1)2^d$, though for diagonal equations the methods of §2 relax this condition to $s > (1+o(1)) d \log d$. However, there is a class of varieties with small dimension relative to degree, for which the circle method supplies non-trivial information concerning the density of rational points. The idea is to apply a descent process in order to interpret points on the original variety in terms of corresponding points on a new variety, with higher dimension relative to degree, more amenable to the circle method.

To illustrate this principle, consider a field extension K of $\mathbb{Q}$ of degree n with associated norm form $N(\mathbf{x}) \in \mathbb{Q}[x_1, \ldots, x_n]$. Also, let l and k be natural numbers with $(k, l) = 1$, and let α be a non-zero rational number. Then Heath-Brown and Skorobogatov [7] descend from the variety $t^l(1-t)^k = \alpha N(\mathbf{x})$ to the associated variety $aN(\mathbf{u}) + bN(\mathbf{v}) = z^n$, for suitable integers a and b. The circle method establishes weak approximation for the latter variety, and thereby it is shown that the Brauer-Manin obstruction is the only possible obstruction to the Hasse principle and weak approximation on any smooth projective model of the former variety. One can artificially construct further examples amenable to the circle method. For example, if we take linearly independent linear forms $L_i(\mathbf{x}) \in \mathbb{Q}[x_1, \ldots, x_n]$ $(1 \le i \le n+r)$, then one can establish non-trivial lower bounds for the density of rational points on the variety $z^k = L_1(\mathbf{x}) \ldots L_{n+r}(\mathbf{x})$ by descending to a variety that resembles a system of r diagonal forms of degree k, with constrained varying coefficients. The investigation of such matters will likely provide an active area of research into the future. In this context we point to work of Peyre [13], which addresses the interaction between descent and the circle method in some generality.

References

[1] B. J. Birch, Forms in many variables, *Proc. Roy. Soc. Ser. A* 265 (1962), 245–263.

[2] J. Brüdern, On pairs of diagonal cubic forms, *Proc. London Math. Soc.* (3) 61 (1990), 273–343.

[3] J. Brüdern, K. Kawada and T. D. Wooley, Additive representation in thin sequences, I: Waring's problem for cubes, *Ann. Sci. École Norm. Sup.* (4) 34 (2001), 471–501.

[4] J. Brüdern and T. D. Wooley, The Hasse principle for pairs of diagonal cubic equations (to appear).

[5] D. R. Heath-Brown, A new form of the circle method, and its application to quadratic forms, *J. Reine Angew. Math.* 481 (1996), 149–206.

[6] D. R. Heath-Brown, Equal sums of three powers (to appear).

[7] D. R. Heath-Brown & A. N. Skorobogatov, Rational solutions of certain equations involving norms, *Imperial College preprint* (June 2001).

[8] C. Hooley, On nonary cubic forms, *J. Reine Angew. Math.* 386 (1988), 32–98.

[9] L.-K. Hua, On Waring's problem, *Quart. J. Math. Oxford* 9 (1938), 199–202.

[10] A. A. Karatsuba, Some arithmetical problems with numbers having small prime divisors, *Acta Arith.* 27 (1975), 489–492.

[11] Ju. V. Linnik, On the representation of large numbers as sums of seven cubes, *Mat. Sb.* 12 (1943), 218–224.

[12] S. T. Parsell, Multiple exponential sums over smooth numbers, *J. Reine Angew. Math.* 532 (2001), 47–104.

[13] E. Peyre, Torseurs universels et méthode du cercle, *Rational points on algebraic varieties, Progr. Math. 199*, Birkhäuser, 2001, pp. 221–274.

[14] W. M. Schmidt, The density of integer points on homogeneous varieties, *Acta Math.* 154 (1985), 243–296.

[15] R. C. Vaughan, A new iterative method in Waring's problem, *Acta Math.* 162 (1989), 1–71.

[16] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge University Press, 1997.

[17] R. C. Vaughan & T. D. Wooley, Further improvements in Waring's problem, III: eighth powers, *Philos. Trans. Roy. Soc. London Ser. A* 345 (1993), 385–396.

[18] R. C. Vaughan & T. D. Wooley, Further improvements in Waring's problem, II: sixth powers, *Duke Math. J.* 76 (1994), 683–710.

[19] R. C. Vaughan & T. D. Wooley, Further improvements in Waring's problem, *Acta Math.* 174 (1995), 147–240.

[20] R. C. Vaughan & T. D. Wooley, Further improvements in Waring's problem, IV: higher powers, *Acta Arith.* 94 (2000), 203–285.

[21] I. M. Vinogradov, The method of trigonometric sums in the theory of numbers, *Trav. Inst. Math. Stekloff* 23 (1947), 109 pp.

[22] I. M. Vinogradov, On an upper bound for $G(n)$, *Izv. Akad. Nauk SSSR Ser. Mat.* 23 (1959), 637–642.

[23] H. Weyl, Über die Gleichverteilung von Zahlen mod Eins, *Math. Ann.* 77 (1916), 313–352.

[24] T. D. Wooley, Large improvements in Waring's problem, *Ann. of Math.* (2) 135 (1992), 131–164.

[25] T. D. Wooley, On Vinogradov's mean value theorem, *Mathematika* 39 (1992), 379–399.

[26] T. D. Wooley, The application of a new mean value theorem to the fractional parts of polynomials, *Acta Arith.* 65 (1993), 163–179.

[27] T. D. Wooley, New estimates for smooth Weyl sums, *J. London Math. Soc.* (2) 51 (1995), 1–13.

[28] T. D. Wooley, Breaking classical convexity in Waring's problem: sums of cubes and quasi-diagonal behaviour, *Invent. Math.* 122 (1995), 421–451.

[29] T. D. Wooley, On exponential sums over smooth numbers, *J. Reine Angew. Math.* 488 (1997), 79–140.

[30] T. D. Wooley, Slim exceptional sets for sums of cubes, *Canad. J. Math.* 54 (2002), 417–448.

[31] T. D. Wooley, Slim exceptional sets in Waring's problem: one square and five cubes, *Quart. J. Math.* 53 (2002), 111–118.

[32] T. D. Wooley, Sums of three cubes, *Mathematika* (to appear).