Notes on Computing Local Densities

Jonathan Hanke

May 14, 2009

1 Computing local densities for a representing a number

1.1 Introduction

Given an integer-valued quadratic form $Q(\vec{x})$ in n variables and an integer m, our goal is to compute the local representation densities

$$\beta_{Q,p}(m) := \lim_{\alpha \to \infty} \frac{r_{Q,p^\alpha}(m)}{p^{\alpha(n-1)}}$$

where $r_{Q,p^k}(m)$ is the number of solutions of $Q(\vec{x}) \equiv m \pmod{p^k}$. We do this by a series of reduction steps based on breaking the solution vectors $\vec{x}$ into various "types" and then counting solutions of some auxiliary quadratic equations $Q'(\vec{x}) \equiv m'$ either mod p (when $p \neq 2$) or mod 8 (when $p = 2$), possibly with additional congruence conditions on $\vec{x}$ (mod p).

1.2 Local Normal Form over $\mathbb{Z}_p$

By an invertible linear change of variables over $\mathbb{Z}_p$ we can always write $Q(\vec{x})$ as a direct sum of quadratic forms with at most two variables (and one variable when $p > 2$) which is referred to as a **Jordan decomposition** of Q. (See cite for details.) Assuming Q is in this form, we group these blocks/subforms by their norm ideal and write

$$Q(\vec{x}) = \bigoplus_{j \in \mathbb{Z}} Q_j(\vec{x}_j)$$

where Q_j is the direct sum of all such subforms of norm ideal (p^j). This decomposition naturally breaks the vector $\vec{x}$ as a tuple of vectors $\vec{x} = (\vec{x}_j)_{j \in \mathbb{Z}}$

Note that our choice of indices j index the norm ideals, and not the scale ideals of the individual blocks, which is slightly non-standard indexing notation. These agree when $p > 2$, but not in general for $p > 2$. However, the choice of indexing by norm is more natural in our context since if Q is integer-valued then we can always take $j \geq 0$ (i.e. $\dim(Q_j) = 0$ if $j < 0$).

In implementing these algorithms it is more convenient to refer to *variables* x_i than Jordan component vectors $\vec{x}_j$ containing those variables (though again they agree when $p = 2$), which we refer to by the variable index i which satisfies $0 \leq i \leq n-1$ where $n = \dim(Q)$. Any conditions we specify on a vector $\vec{x}$ will depend only on the components $\vec{x}_j$, so for each 2×2 block we must refer to either both variables x_i or to neither of them. This applies in particular to the sets $\mathbb{S}$ of indices i described below.

Important Note: All local density reduction algorithms require that Q is written in block diagonal form (with minimal block sizes as described in [3, Lemma 2.1, p355], though the blocks do not need to be strictly ordered by norm or scale.

1.3 Notation and Conventions

1.3.1 Projections of vectors and forms:

For any subset $\mathbb{S} \subseteq \{0, \ldots, n-1\}$ we denote by $\vec{x}_{\mathbb{S}}$ the vector $\vec{x}_{\mathbb{S}} = (x_i)_{i \in \mathbb{S}}$ given by restricting $\vec{x}$ to the components x_i indexed by $\mathbb{S}$ with the standard increasing ordering on indices. We similarly denote $Q_{\mathbb{S}}$ to be direct sum of the subforms using the variables x_i for $i \in \mathbb{S}$. (Note that this is a slightly different convention from [3, p354, ¶4] which refers to the vectors $\vec{x}_{\mathbb{S}} = (\vec{x}_j)_{j \in \mathbb{S}}$ where the index refers to a component of a partition of $\{1, \ldots, n\}$, whereas here the indexing set $\mathbb{S}$ runs over indices $i \in \{0, \ldots, n-1\}$ and not over partition subsets of $\{1, \ldots, n\}$.)

We also often write $\vec{x}_{\mathbb{S}} \equiv \vec{0}_{\mathbb{S}}$ (or $\vec{x}_{\mathbb{S}} \not\equiv \vec{0}_{\mathbb{S}}$) in the slightly abbreviated form $\vec{x}_{\mathbb{S}} \equiv \vec{0}$ (or $\vec{x}_{\mathbb{S}} \not\equiv \vec{0}$) since it is clear from the context that $\vec{0}$ here means $\vec{0}_{\mathbb{S}}$. This convention is consistent with [3,].

1.3.2 Conventions for $\mathbb{S} = \emptyset$:

We also have the standard convention that when $\mathbb{S} = \emptyset$ that $\vec{x}_{\mathbb{S}} \equiv \vec{0}_{\mathbb{S}}$ is trivially true, and so its negation $\vec{x}_{\mathbb{S}} \not\equiv \vec{0}_{\mathbb{S}}$ is always false unless $\mathbb{S} \neq \emptyset$, which is mentioned explicitly in [3, p357, ¶1]. We also adopt the convention that when $\mathbb{S} = \emptyset$ we define $r_{Q_{\mathbb{S}}, p^k}(m) = 1$.

1.3.3 Standard Notation

We denote by $\mathbb{S}, \mathbb{S}_0, \mathbb{S}_1, \mathbb{S}_{2+}, \text{Unit}, \text{NonUnit}, Is8, Not8 \ldots$ sets of indices of variables x_i as described above, which respect the (necessarily given) block decomposition of Q into subforms of dimension ≤ 2.

We let $r_{Q,p^k}(m), r^{Zero, Z \equiv \vec{0}}_{Q,p^k}(m),$ and $r^{Zero, Z \equiv \vec{0}, NZ \not\equiv \vec{0}}_{Q,p^k}(m)$ denote the number of solutions of $Q(\vec{x}) \equiv m \pmod{p^k}$ which respectively satisfy the additional congruence conditions: None, $\vec{x}_Z \equiv \vec{0} \pmod{p}$, and both $\vec{x}_Z \equiv \vec{0} \pmod{p}$ and $\vec{x}_{NZ} \not\equiv \vec{0} \pmod{p}$. Since taking $Z = \emptyset$ is a vacuous condition we see that $r^{Z \equiv \vec{0}}_{Q,p^k}(m)$ can also express $r_{Q,p^k}(m)$, however there are no generically vacuous conditions for NZ so this condition must be explicitly included or not in our formulas. Also while multiple zero congruence conditions $\vec{x}_{Z1} \equiv \vec{0}$

and $\vec{x}_{Z2} \equiv \vec{0}$ can be combined as $\vec{x}_{Z1 \cup Z2} \equiv \vec{0}$ in a single condition, the non-zero congruence conditions cannot be combined. Our notation (and implementation) allows for at most one such non-zero condition, which is either passed in as the class "None" or as a vector of indices for NZ.

1.4 Congruence Conditions

It will be useful to consider representation densities for vectors subject to certain congruence conditions (mod p). These will always be relative to a fixed block diagonal decomposition of Q as described above, and are not well-defined without this choice. These either take the form $\vec{x}_Z \equiv \vec{0}_Z \pmod{p}$ or $\vec{x}_{NZ} \not\equiv \vec{0}_{NZ} \pmod{p}$ or both, for some sets of indices Z and $NZ \subseteq \{0, \ldots, n-1\}$. (It happens that for our purposes we will not need to have more than one non-zero congruence condition, and any number of zero congruence conditions are equivalent to a single larger one.)

There are two main observations for computing the densities subject to the conditions $\vec{x}_Z \equiv \vec{0}$ and $\vec{x}_{NZ} \not\equiv \vec{0}$:

1. $(\vec{x}_Z \equiv \vec{0}, \vec{x}_{NZ} \not\equiv \vec{0}) = (\vec{x}_Z \equiv \vec{0}) - (\vec{x}_{Z \cup NZ} \equiv \vec{0})$
2. The above formula counts no solutions when $NZ \subseteq Z$, so when this happens we declare there are no solutions.

1.5 Counting Solutions in $\mathbb{F}_p$ for primes $p \neq 2$

Assuming the Jordan block form above, we are interested in computing the number of solutions $r_{Q,p}(m)$ of $Q(\vec{x}) = m$ in $\mathbb{F}_p$. If we denote the $j = 0$ (unit scale) indexing set by Unit, and the other (non-unit scale) indices $j > 0$ by NonUnit, then reducing the Jordan form mod p gives the formulas

$$r_{Q,p}(m) = r_{Q_{\text{Unit}},p}(m) \cdot p^{|\text{NonUnit}|}$$

$$r_{Q,p}^{Z \equiv \vec{0}}(m) = r_{Q_{\text{Unit}-(\text{Unit} \cap Z)},p}(m) \cdot p^{|\text{NonUnit}|-|\text{NonUnit} \cap Z|} \tag{1}$$

since the components $\vec{x}_{\text{NonUnit}}$ can be freely chosen. Notice that this formula also holds with the convention that when $\mathbb{S} = \emptyset$ we set $r_{Q_{\mathbb{S}}}(m) = 1$. By combining this with the method of dealing with non-zero congruence conditions described in subsection 1.4, we obtain the final formula for both zero and non-zero congruence conditions as:

$$r_{Q,p}^{Z \equiv \vec{0}, NZ \not\equiv \vec{0}}(m) = r_{Q_{\text{Unit}-(\text{Unit} \cap Z)},p}(m) \cdot p^{|\text{NonUnit}|-|\text{NonUnit} \cap Z|} \tag{2}$$

$$- r_{Q_{\text{Unit}-(\text{Unit} \cap (Z \cup NZ))},p}(m) \cdot p^{|\text{NonUnit}|-|\text{NonUnit} \cap (Z \cup NZ)|} \tag{3}$$

To evaluate $r_{Q,p}(m)$ when $Q = Q_{\text{Unit}}$ we have the following formulas from the theory of Gauss sums for a non-degenerate quadratic form Q of Gram determinant D (hence D

is non-zero) over $\mathbb{F}_p$:

$$r_{Q,p}(m) = \begin{cases} p^{n-1} & \text{if } n \text{ is odd and } m \equiv 0 \pmod{p} \\ p^{n-1} + p^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} D\, m}{p} \right) & \text{if } n \text{ is odd and } m \not\equiv 0 \pmod{p} \\ p^{n-1} + p^{\frac{n-2}{2}} (p-1) \left(\frac{(-1)^{\frac{n}{2}} D}{p} \right) & \text{if } n \text{ is even and } m \equiv 0 \pmod{p} \\ p^{n-1} - p^{\frac{n}{2}} \left(\frac{(-1)^{\frac{n}{2}} D}{p} \right) & \text{if } n \text{ is even and } m \not\equiv 0 \pmod{p} \end{cases}$$

See [1,] or [2,] for the general formulas, and [3, Table 1, p363] for when $n \leq 4$.

1.6 Counting Good-type Solutions for $p \neq 2$

Definiton 1.1. *We say that a solution vector $\vec{x}$ of $Q(\vec{x}) \equiv m \pmod{p^k}$ is of* **Good-type** *solutions (for odd primes p) if $a_{ii}x_i \neq 0$ for some index i.*

We define indexing sets Unit and NonUnit to give the variable indices where a_{ii} is (resp. is not) a unit mod p. In terms of the Jordan decomposition, the Good-type condition can be stated equivalently as saying that $\vec{x}_{\text{Unit}} \not\equiv \vec{0}$.

If $m \not\equiv 0 \pmod{p}$ then $r^{Good}_{Q,p}(m) = r_{Q,p}(m)$ since some component of $\vec{x}_{\text{Unit}}$ must be non-zero. The same formula also holds if we add any additional congruence conditions to both sides.

If $m \equiv 0$ then we can add the Good-type requirement to both sides of equations (1) or (2) to obtain a formula. Since the "type" condition on a solution vector $\vec{x}$ is independent of any additional congruence conditions imposed on it, we are reduced to equation (2) where both terms on the RHS count only Good-type solutions. This happens for each term individually when $\vec{x}_{\text{Unit}} \neq \vec{0}$ for each solution vector, so when $m = 0$ we need to subtract off the zero vector, giving either

$$r^{Good, Z \equiv \vec{0}}_{Q,p}(0) = (r_{Q_{\text{Unit}-(\text{Unit}\cap Z)},p}(0) - 1) \cdot p^{|\text{NonUnit}|-|\text{NonUnit}\cap Z|}$$

or

$$\begin{aligned} r^{Good, Z \equiv \vec{0}, NZ \not\equiv \vec{0}}_{Q,p}(0) = {} & (r_{Q_{\text{Unit}-(\text{Unit}\cap Z)},p}(0) - 1) \cdot p^{|\text{NonUnit}|-|\text{NonUnit}\cap Z|} \\ & - (r_{Q_{\text{Unit}-(\text{Unit}\cap (Z\cup NZ))},p}(0) - 1) \cdot p^{|\text{NonUnit}|-|\text{NonUnit}\cap (Z\cup NZ)|}. \end{aligned}$$

1.7 Counting Good-type Solutions for $p = 2$

When $p = 2$ to compute local densities by lifting Good-type solutions we must count solutions mod 8 (not just mod 2). Since $\mathbb{Z}/8\mathbb{Z}$ is not field we do not have a Gauss sum which quickly computes the number of solutions, and we resort to just counting solutions

naively (i.e. one at at time) according to their solution type and auxiliary congruence conditions. (**Note:** This can possibly be sped up by some fixed linear factor by caching various representation numbers of small dimensional forms mod 8, but this is not done currently.)

The only simplification we make is to simplify the dependence of the answer on the Jordan blocks whose norm is divisible by 8. If we denote by $Not8$ and $Is8$ the sets of indices of Jordan blocks whose norms respectively aren't and are divisible by 8, then we have the two formulas:

$$r_{Q,8}^{Good,Z\equiv\vec{0}}(m) = r_{Q_{Not8},8}^{Good,Z\cap Not8\equiv 0}(m)\cdot 4^{|Is8\cap Z|}\cdot 8^{|Is8|-|Is8\cap Z|}$$

and

$$r_{Q,8}^{Good,Z\equiv\vec{0},NZ\not\equiv\vec{0}}(m) = r_{Q,8}^{Good,Z\equiv\vec{0}}(m) - r_{Q,8}^{Good,Z\cup NZ\equiv\vec{0}}(m)$$

where the last formula can be worked out explicitly in terms of the first formula.

1.8 Counting Zero-type Solutions

Definiton 1.2. *A solution $\vec{x}$ of $Q(\vec{x}) \equiv m \pmod{p^k}$ is said to be of* **Zero-type** *if $\vec{x} \equiv \vec{0} \pmod{p}$.*

Note that a necessary condition for such a solution to exist is that $p^2 \mid m$, since $\vec{x} = p\vec{x}' \implies m = Q(\vec{x}) = Q(p\vec{x}') = p^2Q(\vec{x}')$. From the definition, we see that the extra congruence conditions for Zero-type solutions are easily dealt with by the formulas

$$r_{Q,p^k}^{Zero,Z\equiv\vec{0}}(m) = r_{Q,p^k}^{Zero}(m) \qquad \text{and} \qquad r_{Q,p^k}^{Zero,Z\equiv\vec{0},NZ\not\equiv\vec{0}}(m) = 0.$$

From [3, p359] we know that there is a surjective map

$$\pi_Z : R_{Q,p^k}^{Zero}(m) \to R_{Q,p^{k-2}}(m/p^2)$$

with multiplicity p^n, and taking $k >> 1$ gives the reduction formula

$$\beta_{Q,p}^{Zero}(m) = \frac{r_{Q,p^k}^{Zero}(m)}{p^{(n-1)k}} = \frac{r_{Q,p^{k-2}}(m/p^2)\cdot p^n}{p^{(n-1)k}} = \frac{r_{Q,p^{k-2}}(m/p^2)\cdot p^{n-2(n-1)}}{p^{(n-1)(k-2)}} = \tfrac{1}{p^{n-2}}\beta_{Q,p}(m/p^2).$$

Thus we can reduce our computation of Zero-type solutions representing m to arbitrary solutions representing m/p^2.

1.9 Counting Bad-type I Solutions

We define the indexing sets

$$\begin{aligned}
\mathbb{S}_0 &= \{i \mid 0 \le i < n, x_i \text{ is a variable in } \vec{x}_0 \text{ (or in } Q_0)\} \\
\mathbb{S}_1 &= \{i \mid 0 \le i < n, x_i \text{ is a variable in } \vec{x}_1 \text{ (or in } Q_1)\} \\
\mathbb{S}_{2+} &= \{i \mid 0 \le i < n, x_i \text{ is a variable in } \vec{x}_j \text{ (or in } Q_j) \text{ for some } j \ge 2\}
\end{aligned}$$

of sizes $s_0, s_1,$ and s_{2+} respectively. Also let $\mathbb{S}_{\ge 1} := \mathbb{S}_1 \cup \mathbb{S}_{2+}$.

Definiton 1.3. *In terms of these sets, we can define the Bad-type I solutions to be those not of Good-type or Zero-type for which* $\vec{x}_{\mathbb{S}_1} \not\equiv \vec{0} \pmod{p}$.

A necessary condition for these to exist is that $p \mid m$ and $\vec{x}_{\mathbb{S}_1} \not\equiv \vec{0} \pmod{p}$. From [3, p360] we know that there is a surjective map

$$\pi_{B'} : R^{BadI}_{Q,p^k}(m) \to R^{Good}_{Q',p^{k-1}}(m/p)$$

for some auxiliary form Q' and this map has multiplicity $p^{s_1+s_{2+}}$.

Under $\pi_{B'}$, congruence conditions $Z \equiv \vec{0}$ restrict to $Z \cap (\mathbb{S}_1 \cup \mathbb{S}_{2+}) \equiv \vec{0}$ and $NZ \not\equiv \vec{0}$ restrict to $NZ \cap (\mathbb{S}_1 \cup \mathbb{S}_{2+}) \not\equiv \vec{0}$ (and this also holds true when the index intersection is $\emptyset$). Therefore we have that

$$r^{BadI, Z\equiv\vec{0}, NZ\not\equiv\vec{0}}_{Q,p^k}(m) = p^{s_1+s_{2+}} \cdot r^{Good, Z\cap\mathbb{S}_{\geq 1}\equiv\vec{0}, NZ\cap\mathbb{S}_{\geq 1}\not\equiv\vec{0}}_{Q',p^{k-1}}(m/p)$$

and similarly with no non-zero congruence condition on both sides. By taking $k >> 1$ we obtain the local density reduction formula

$$\begin{aligned}\beta^{BadI,C}_{Q,p}(m) &= \frac{r^{BadI,C}_{Q,p^k}(m)}{p^{(n-1)k}} = \frac{p^{s_1+s_{2+}} \cdot r^{Good,C\cap\mathbb{S}_{\geq 1}}_{Q',p^{k-1}}(m/p)}{p^{(n-1)k}} \\ &= \frac{p^{s_1+s_{2+}-(n-1)} \cdot r^{Good,C\cap\mathbb{S}_{\geq 1}}_{Q',p^{k-1}}(m/p)}{p^{(n-1)(k-1)}} = p^{1-s_0} \cdot \beta^{Good,C\cap\mathbb{S}_{\geq 1}}_{Q,p}(m/p).\end{aligned}$$

Remark 1.4 (**Notational Note**). In the above formula we are using the shorthand "$C \cap \mathbb{S}$" for "$Z \cap \mathbb{S} \equiv \vec{0}, NZ \cap \mathbb{S} \not\equiv \vec{0}$", and also the indexing set $\mathbb{S}_{\geq 1}$ is defined relative to the original form Q (not the new form Q').

Remark 1.5 (**Ordering Warning**). The Bad-type I reduction procedure does not preserve the "increasing valuation" ordering of the block diagonal local normal form! This is important to notice because it means that we should not depend on this property of our block diagonal quadratic form which is then passed as input to other local density congruence routines!

1.10 Counting Bad-type II Solutions

Another definition of the Bad-type II solutions are is that they are Bad-type solutions where $\vec{x}_{\mathbb{S}_1} \equiv \vec{0}$. For there to be solutions, we must have that $\mathbb{S}_{2+} \neq \emptyset$ (or more generally that $\vec{x}_{\mathbb{S}_{2+}} \not\equiv \vec{0}$) and that $p^2 \mid m$.

We then obtain a reduction formula which returns a reduction formula to solutions which satisfy the congruence conditions $Z \cap \mathbb{S}_{2+} \equiv \vec{0}$, $NZ \cap \mathbb{S}_{2+} \not\equiv \vec{0}$, and also $\vec{x}_{\mathbb{S}_{2+}} \not\equiv \vec{0}$. The presence of *two* non-zero congruence conditions does not fit into our current implementation

framework (which accommodates at most one non-zero congruence condition), though this can be dealt with by

$$(C \cap \mathbb{S}_{2+}, \vec{x}_{\mathbb{S}_{2+}} \not\equiv \vec{0}) \quad = \quad (Z \cap \mathbb{S}_{2+} \equiv \vec{0}, NZ \cap \mathbb{S}_{2+} \not\equiv \vec{0}) - (\mathbb{S}_{2+} \cup (Z \cap \mathbb{S}_{2+}) \equiv \vec{0}, NZ \cap \mathbb{S}_{2+} \not\equiv \vec{0}).$$

Here the second zero congruence can be simplified since $\mathbb{S}_{2+} \cup (Z \cap \mathbb{S}_{2+})$ is just $\mathbb{S}_{2+}$.

References

[1] A. I. Borevich and I. R. Shafarevich. *Number theory.* Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[2] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs.* Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[3] Jonathan Hanke. Local densities and explicit bounds for representability by a quadratic form. *Duke Math. J.*, 124(2):351–388, 2004.