AFFINE SIEVE

PETER SARNAK (June 2010)

§0. Brief History:

The affine sieve refers not to a new combinatorial sieve but rather a new setting in which the classical sieve of Brun as well as some other sieves can be executed.

For me the starting point of this investigation was in 2005 when Michel and Venkatesh asked me about the existence of poorly distributed closed geodesics on the modular surface. It was clear that Markov's constructions

of his geodesics using his Markov[1] equation (see page 6 below) provided what they wanted but they prefered quadratic forms with square free discriminant. This raised the question of sieving in this context of an orbit of a group of (nonlinear) morphisms of affine space. The kind of issues that one quickly faces in attempting to execute such a sieve are questions of the image of the orbit when reduced mod q and interestingly whether certain graphs associated with these orbits are expander families. Gamburd

in his thesis had established the expander property in some simpler but similar settings and he and I began a lengthy investigation into this sieving problem in the simpler setting when the group of affine morphisms acts linearly (or what we call now the affine linear sieve).

Thanks to contributions by many people (some key references are listed below) the affine linear sieve is today in good shape. In §2 we describe this setting and applications of a 'Brun' combinatorial sieve. Applications of more general

affine linear sieves (eg a large sieve) to geometric and irreducibility questions have been developed recently by Rivin and Kowalski. One striking feature of the affine sieve, are the different tools from geometry, group theory, combinatorics and of course number theory that are used in executing the sieve.

References:

(1) [B-G-S] ~~"Affine"~~ J. Bourgain, A. Gamburd, P. Sarnak "Affine linear sieve, expanders and sum product" Invent. Math (2010) 179, 559-644

(2). [N-S] A. Nevo and P. Sarnak "Prime and Almost prime points a principal homogeneous spaces" Acta Math to appear

(3) [H] H. Helfgott Annals of Math 167 (2008) 601-623

(4). [B-G] J. Bourgain and A. Gamburd Annals of Math 167 (2008) 625-642

(5) [R] I. Rivin "Counting ~~irreducible~~ matrices, polynomials, surface and free groups" ArXiv (2006)

(6) [K] E. Kowalski "The large sieve and its applications" Arithmetic geometry random walks and discrete groups. CUP, 175 (2008)

(7) [V] P. Varju "Expansion in $SL_d(\mathcal{O}/I)$, I square free" ArXiv 2010

(8) [P-Z] L. Pyber and E. Szabo "Growth in finite groups of Lie type" ArXiv 2010.

(9) [B-G-T] E. Breuillard, B. Green and T. Tao "Linear approximate groups" ArXiv 2010

(10) [B-K] J. Bourgain and A. Kontorovich "Integers in Thin subgroups of $SL_2(\mathbb{Z})$" ArXiv 2010

(11) [S] P. Sarnak "Integral Apollonian packings" WWW.math.princeton.edu/sarnak

§1: Affine Sieve

Classical combinatorial sieve BRUN:

$f \in \mathbb{Q}[x]$, $f(\mathbb{Z}) \subset \mathbb{Z}$ and f primitive: for $q \geq 1$ there is x s.t. $(f(x), q) = 1$.

Want to find x's (many) with $f(x)$ prime or at least as few as possible prime factors.

- Define the saturation number

$$\tau_0(\mathbb{Z}, f) = \tau_0(f)$$

= smallest τ such that the set of x for which $f(x)$ is a product of at most τ primes is infinite.
(if no such τ exist $\tau_0 = \infty$).

Eg: (1) $f(x) = x$, $\tau_0(f) = 1$

$\Leftrightarrow$ there infinitely many primes.

(2) $f(x) = ax+b$, $(a,b)=1$

$\tau_0(f) = 1$; there are infinitely primes in a progression.

τ_0 is not known for $\deg(f) = d > 1$.

(3). $\tau_0(x(x+2)) = 2$ iff twin prime conj. holds

(4) $\tau_0(x^2+1) = 1 \Leftrightarrow$ Euler conjecture.

Fundamental Theorem (BRUN):

$\tau_0(\mathbb{Z}, f) < \infty$ in fact the bound depends only on $d = \deg f$ and $t = \#$ of irreducible factors of $f/\mathbb{Q}$.

Eg: $\tau_0(x(x+2)) \leq 20$

improvements ....

Chen (± 1970):

$$\tau_0(\mathbb{Z}, x(x+2)) \le 3.$$

Iwaniec (1972):

$$\tau_0(\mathbb{Z}, x^2+1) \le 2$$

Halberstam-Richert (1970's):

f irreducible over $\mathbb{Q}$, $d = \deg f$

$$\tau_0(\mathbb{Z}, f) \le d+1.$$

The main idea of BRUN is to truncate the inclusion/exclusion process in sieving; striking out multiples of 2, 3, ... adding back multiples of 6, ... and to still give upper and lower bounds for what remains.

- Key point is it reduces to counting integers in progressions

$$|\{x \in \mathbb{Z} : |x| \le N, x \equiv a \pmod q\}| = \frac{2N}{q} + O(1).$$

This can be generalized to several variables:

$$f \in \mathbb{Q}[x_1, \ldots, x_n], \quad f(\mathbb{Z}^n) \subset \mathbb{Z}$$
primitive

$$\tau_0(\mathbb{Z}^n, f)$$

Asks for the least τ such that $f(x)$ is a product of at most τ primes on a Zariski dense set of x's in $\mathbb{A}^n$.

Zariski density is the natural algebraic extension of 'infinitely many' in $\mathbb{A}^1$.

- One can replace $\mathbb{Z}^n$ above by a subset such as $V(\mathbb{Z})$ where $V/\mathbb{Q}$ is an algebraic variety. However in such generality one quickly runs into problems of Hilbert's 10-th problem.

The setting in which things have taken off recently is when the subset is an orbit $\mathcal{O}$ of a group of affine motions: The "affine sieve".

Γ a group of affine morphisms (polynomial maps) of $\mathbb{A}^n$ which take $\mathbb{Z}^n$ to $\mathbb{Z}^n$.

$$\mathcal{O} = a \cdot \Gamma \subset \mathbb{Z}^n \quad \text{(act on right)}$$

$$f \in \mathbb{Q}[x_1, x_2, \ldots x_m], \quad f|_{\mathbb{Z}^n} \subset \mathbb{Z}$$

f primitive on $\mathcal{O}$.

Seek $\ll$ many points $x \in \mathcal{O}$ for which $f(x)$ has at most r - prime factors, these points should be Zariski dense in $Zcl(\mathcal{O}) \subset \mathbb{A}^m$.

$\rightarrow$ $r_0(\mathcal{O}, f)$ the saturation number of f on $\mathcal{O}$.

Why ask?

Examples:

(1) Markoff Numbers (my original motivation for an affine sieve)

$$V: \quad x^2+y^2+z^2 = 3xyz \quad \subset \mathbb{A}^3$$

$V(\mathbb{Z})$?

Let Γ be the group of affine morphisms of $\mathbb{A}^3$ generated by the involutions R_j $(R_j^2 = 1)$

$$R_1(x,y,z) = (3xy-x, y, z)$$
$$R_2(x,y,z) = (x, 3xz-y, z)$$
$$R_3(x,y,z) = (x, y, 3xy-z)$$

$\Gamma(\mathbb{Z}^n) = \mathbb{Z}^n$.

Markoff: $V(\mathbb{Z}) = (1,1,1).\Gamma$ (proof by descent)

Can we sieve on $V(\mathbb{Z})$?
Are there infinitely (or Zariski dense) set of $(x,y,z) \in V(\mathbb{Z})$ with x square-free?

Note: R_j's are nonlinear.

Eg 2: (Pythagorean Triples)

$\mathbb{A}^3$. $V: \quad x^2+y^2-z^2=0$

$$F(x,y,z) = x^2+y^2-z^2$$

V cone: $F=0$.

$G = O_F$ the orthogonal group of F, all 3×3 matrices preserving F.

$\Gamma = G(\mathbb{Z})$ those with integer entries

"arithmetic linear alg. group".

$$V^{prim}(\mathbb{Z}) = (3,4,5)\Gamma = \mathcal{O}$$

= all primitive pythagorean triples.

Let $f = \frac{xy}{12} = \text{Area}/6$ is primitive integral on $\mathcal{O}$

What is $\tau_\bullet(\mathcal{O}, f)$?

i.e. what is the least number of prime factors that the areas of a full (Zariski dense) set of pythag. triples can have?

Eg 3: Integral Apollonian packings:

$$F(x_1,x_2,x_3,x_4) = 2(x_1^2+x_2^2+x_3^2+x_4^2) - (x_1+x_2+x_3+x_4)^2$$

Descartes quadratic form.

$G = O_F$

$O_F(\mathbb{Z})$ 'arithmetic group'

- A the "Apollonian group"

$$A = \langle S_1, S_2, S_3, S_4 \rangle, \quad S_j^2 = 1$$

$$S_1 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix}, \quad S_4 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

- $A \leq O_F(\mathbb{Z})$ is of <u>infinite</u> index
- $\overline{Zcl(A) = O_F}$. "NON ARITHMETIC" OR THIN

(9)

(-11, 21, 24, 28)
starting 4 circles tangent

integers are the curvatures of the circles

An Integral Apollonian packing

$a = (-11, 21, 24, 28)$

$F(a) = 0$ [in fact Descartes' theorem asserts that any 4 mutually tangent circles have their curvatures satisfy $F(\quad) = 0$]

$$\mathcal{O}_a = a \cdot \Gamma \subset \mathbb{Z}^4$$

consists of all $\overset{4}{\wedge}$ mutually tangent circles in the packing.

Are there infinitely many circles whose curvature is prime? Pairs of circles both of whose curvatures are prime?

- $\tau_0(\mathcal{O}_a, f)$ $f(x) = x_1$, $f(x) = x_1 x_2$.

Many geometric constructions of affine linear groups lead to Γ being "thin".

Can we execute a combinatorial sieve in the affine (linear) setting? Is the saturation number always finite?

Enemy: TORUS

action $x \to xa + b$, $a \in GL_n(\mathbb{Z})$, $b \in \mathbb{Z}^n$

if $a = 1$, $x \to x + b$ translations orbits are linear subspaces – no problem to execute a BRUN sieve. The trouble is multiplication.

- Pure multiplication:

$n = 2$ $\quad \Gamma = \left\{ \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix}^m : m \in \mathbb{Z} \right\} \leq SL_2(\mathbb{Z})$

$Zd(\Gamma)$ is a $\mathbb{Q}$-torus.

$\mathcal{O} = (1,0)\Gamma = \{ (F_{2n}, F_{2n-2}) : n \in \mathbb{N} \}$

F_n the n-th Fibonacci no!

$$Zcl(\Theta) = \{(x_1, x_2) : x_1^2 - 3x_1x_2 + x_2^2 = 1\}$$

standard heuristics suggest that

$$\tau_0(\Theta, f) = \infty . \qquad !$$

No saturation.

Main new development:

$\Gamma \leq GL_m(\mathbb{Z})$ (linear group)

$G = Zcl(\Gamma)$ linear algebraic group.

Key assumption is that $rad(G)$ (the largest normal solvable algebraic subgroup) contains no tori.

(*)

↓ the radical

Fundamental theorem of the affine (linear) sieve:

Under (*) $\tau_0(\theta, f) < \infty$ for any Γ orbit θ and any $f \in \mathbb{Q}[x_1, \ldots, x_n]$.

This is not written up in general as yet and it is a consequence of many works

- Bourgain-Gamburd-S, general set up and analysis and proof for $G = SL_2$ (2009)
- proof for SL_2 depends on Helfgott's combinatorial A.A.A theorem in $SL_2(\mathbb{F}_p)$
- Pyber-Szabo, Breuillard-Green-Tao extend Helfgott to general G. (2010)
- P. Varju extends B-G-S expander theorem to SL_n
- Salehi-Varju, extend expander theorem for general G.

In general no bounds for $T_0(\mathcal{O}, f)$ are provided by the proof.

If Γ is arithmetic (i.e. finite index in the $\mathbb{Z}$-points of $Zcl(\Gamma)$) Then one can use automorphic forms specifically "Ramanujan Conjectures"

- Nevo-S (2009): give bounds for $T_0(\mathcal{O}, f)$ depending only on $d = \deg f$ and t no' of irreducible components of f in the coord ring $\mathbb{R}[Zcl(\mathcal{O})]$, which are essentially as good as what is known for the 1-variable BRUN sieve.

Gems for which one can determine $\tau_0(\mathcal{O}, f)$ & exactly:

(i) Pythagorean triples

$$\mathcal{O} = (3,4,5)\, O_f(\mathbb{Z}) \subset \mathbb{Z}^3$$

- $\tau_0\left(\mathcal{O}, \frac{x_1 x_2}{12}\right) = 4$

that is the minimum number of factors that the area of a Zariski dense set of pythagorean triangles can have is 4 (we remove the forced factor of 3 and 2).

Proof: (exercise)

first use the ancient parametrization of such triples $\mathbb{A}^2 \longrightarrow V$

then apply the very recent breakthrough of Green and Tao that one can solve 2 simultaneous linear equation in 4 prime variables.

Theorem (S, 07):

$\mathcal{O} = a \cdot A$, Apollonian group.

$\Leftrightarrow$ integral apollonian packing

$$\tau_0(\mathcal{O}_a, x_1) = 1$$

$$\tau_0(\mathcal{O}_a, x_1 x_2) = 2$$

$\Rightarrow$ there are infinitely circles with curvature a prime and there are infinitely many pairs of tangent circles both of whose curvatures are prime.

Why is the affine sieve so much more difficult than the classical BRUN sieve?

One executes a delicate inclusion process on $\mathcal{O}$ or better still, directly on Γ

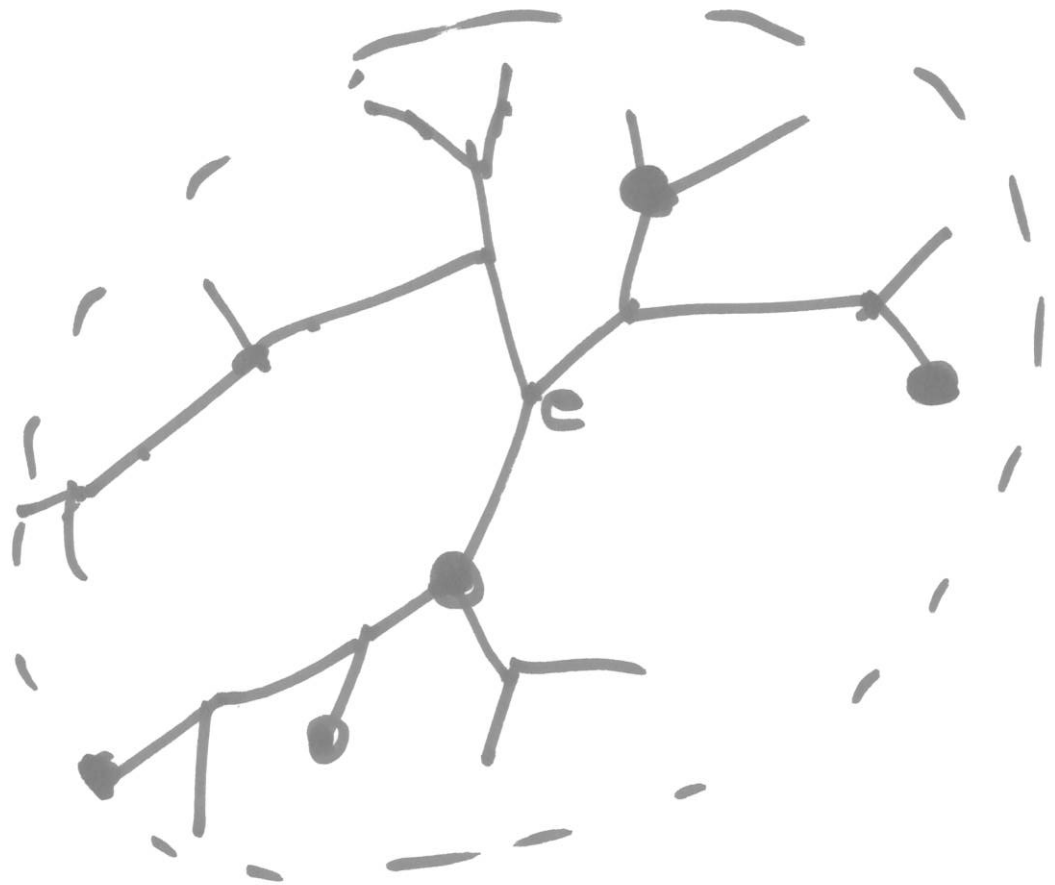
Introduce an ordering $\| \ \|$ on Γ count

$\|x\| \leq T$

$f(x) \equiv 0 \pmod{d}$

or $x \equiv a \pmod{d}$.

"tree-like" (different to $\mathbb{Z}^4$).



Γ

price of multiplicati + additi

# of points $\|x\| \leq T$

$\approx \|x\| \leq T$ on bdry

plus congruence.

- Need a version of strong approximation

$$\Gamma \longrightarrow \Gamma(\text{mod } d) \quad \text{image}$$

[Weisfeiller; Matthews Vaserstein Nori, Larsen-Pink ⊥

- need the related Cayley graphs to be "expanders".

eg: $\Gamma \leq SL_2(\mathbb{Z})$, Γ Zariski dense in SL_2.

$$\Gamma \xrightarrow[\text{onto}]{\text{mod } p} SL_2(\mathbb{Z}/p\mathbb{Z}), \quad p \text{ large}$$

S a symmetric gen set for Γ

$X_p = (SL_2(\mathbb{Z}/p\mathbb{Z}), S)$

Cayley graphs - expanders. ...