COLUMNS FROM A SPHERE

Prerequisites. Linearity of expectation, the union bound and Chebyshev's inequality for sums of independent Bernoulli variables. From Chapter 4, *Fourier analysis on the Galois group*: the group H, the cells $\mathrm{cell}_t(r)$ and Problem 4.1.3 (Section 4.1), and the thick cells Θ_u, the density $\delta = |T_2|/n$ and Theorem 4.4.1 (Section 4.4).

In Chapter 4 a set T_2 of columns was fixed, and the cells of row 1 in the columns uT_2 were given the weight b, so that they test primes near x. Nothing was asked of T_2 there except that it be large: Theorem 4.4.1 divides by δ. How is T_2 chosen? The argument asks for a second property, that the cells of the odd powers of one prime rarely fall in uT_2, and the two properties pull in opposite directions. Behrend's construction [Beh] satisfies both: lattice points on a sphere, written as digits in a large base. We follow [Rub, §III.3] and [Adr, §5].

Throughout, x is large, $0 < \varepsilon < \frac{1}{52}$, and n is a power of 2 with $x^{2+8\varepsilon} \le n \le 2x^{2+8\varepsilon}$; the notation $q, d, N = 4n, H, \Phi, v(r)$ is that of Chapter 4. The integer $L \ge 2$ is at most $C_L \log x$ for a constant C_L; in the argument L is of order $\log x$ [Rub, §III.3].

5.1. Two requirements

Problem 5.1.1. The group $H = (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ is cyclic of order n, generated by $[5]$. For $N = 16$, $[5]^0, [5]^1, [5]^2, [5]^3$ are $[1], [5], [7], [3]$.

We write H additively through $\iota\colon H \to \mathbb{Z}/n\mathbb{Z}$, $\iota([5]^i) = i$, and regard a set of integers $T_2 \subset [0, n)$ as the set of columns $\{[5]^s : s \in T_2\}$. Then the thick cells for the translate u are the cells in row 1 whose column c has $\iota(c) \in \iota(u) + T_2$.

Problem 5.1.2. Let p be a prime inert in $K = \mathbb{Q}(\sqrt{-d})$, $p \nmid 2qd$, and $\iota_p := \iota([p])$. For odd $h \ge 1$ and $t \in H$, the cell $\mathrm{cell}_t(p^h)$ is in row $v(p)$ and its column has index $\iota(t) + h\iota_p$. So the cells of $p, p^3, p^5, \dots$ run along the progression $\iota(t) + \iota_p + 2\iota_p\,\mathbb{Z}$ in a single row.

We call these the *Frobenius progressions*. The first requirement on T_2 comes from averaging.

Problem 5.1.3. Let r be a prime power with a cell, and $t \in H$. The number of $u \in H$ for which $\mathrm{cell}_t(r)$ is thick for w_u is $|T_2|$ if $v(r) = 1$, and 0 if $v(r) = 0$.

So the average over translates sees T_2 only through δ, and every prime power of row 1 gets the weight δ; this is Problem 4.4.3. The gain of the argument is proportional to δ, while its errors are not, and in Theorem 4.4.1 the mean excess is divided by δb. The argument needs

$$\delta \ge x^{-\varepsilon}, \tag{1}$$

which is used in the chapter *Assembly at one scale*, where the other losses are also powers $x^{O(\varepsilon)}$.

Date: November 25, 2026.

The second requirement concerns a single translate. For all $u, t \in H$ and every prime as in Problem 5.1.2, at most two of the cells of L consecutive odd powers p^h may be thick, provided $2\iota_p$ has order greater than $4L$. If the order is at most $4L$, at most one cell of any odd power of p may be thick. In [Rub] the sets of columns enter the main inequality through (1) and through a bound for the losses at inert primes, which is quoted there from the formal proof [Rub, §III.6]. These are losses of the kind in Theorem 17.3.1 of Chapter 17, the weight w subtracted at each odd level, not the colength of Chapter 19: at the scale p^h the loss is at most w, where w is the weight of the cell to which Frobenius links the chosen one [Rub, §I.4.3], and a thick cell carries the large weight b. This second property is the form in which T_2 is recorded for that bound, which we do not treat here. The requirement is uniform: it must hold for every u, t and p, with no exceptions.

Why are these two requirements in tension? The obvious sets of integers without three-term progressions are thin.

Problem 5.1.4. Let A_k be the set of integers in $[0, 3^k)$ whose base-3 digits are 0 or 1. (i) A_k contains no three-term arithmetic progression, and $|A_k| = (3^k)^{\log 2/\log 3}$. (ii) For $k \geq 2$, A_k contains $0, 1, 3$, and $3(1-0) = 1 \cdot (3-0)$.

As a set of columns with $n \approx 3^k$, A_k has density $n^{-0.369\cdots}$, far below $x^{-\varepsilon}$. A random set has the right density but meets progressions too often.

Problem 5.1.5. Let $R \subset \mathbb{Z}/n\mathbb{Z}$ contain each element independently with probability δ. The expected number of pairs (s, h) with $s, s+h, s+2h \in R$ and h of order greater than $4L$ is at least $n(n-4L)\delta^3$. For $\delta = x^{-\varepsilon}$ this exceeds $\delta n \cdot x^2$ for large x.

Each such pair gives three consecutive terms $s, s+h, s+2h$ of a progression in R, against the second requirement for every $L \geq 3$. In expectation there are far more bad pairs than points of R, so counting one deleted point for each bad pair leaves no lower bound for what survives. The count alone does not show that no cleverer deletion succeeds, since one point can lie on many bad pairs; but it locates the density at which the naive deletion stops working.

Problem 5.1.6. Let R be as in Problem 5.1.5, and let R' be obtained by deleting one point from each bad pair. Then R' contains no bad pair, and its expected size is at least $\delta n - \delta^3 n^2$. For $\delta \leq (2n)^{-1/2}$ this is at least $\delta n/2$, and $(2n)^{-1/2} < x^{-1-4\varepsilon}$.

So a random set with deletions reaches a density about $n^{-1/2}$, and to raise it to $x^{-\varepsilon}$ the set must be built with structure.

5.2. Behrend's construction

Three points of a sphere are never collinear. Behrend's idea is to transport this to the integers by writing vectors as digits. Let $S, D \geq 2$ be integers and $\Sigma_k := \{v \in \{0, \dots, D-1\}^S : |v|^2 = k\}$.

Problem 5.2.1. Let v_1, v_2, v_3 lie on one sphere $|v|^2 = k$ in $\mathbb{R}^S$, and let i, j be real with $i, j \neq 0$, $i \neq j$ and $j(v_2 - v_1) = i(v_3 - v_1)$. Then $v_1 = v_2 = v_3$.

Problem 5.2.2. Some k has $|\Sigma_k| \geq D^{S-2}/S$.

Fix such a k. Let $B := 4LD$, $s(v) := \sum_{m=0}^{S-1} v_m B^m$, and $T_2 := s(\Sigma_k)$.

Problem 5.2.3. If $c_0, \dots, c_{S-1}$ are integers with $|c_m| < B$ and $\sum_m c_m B^m = 0$, then every $c_m = 0$. In particular s is injective.

Problem 5.2.4. There are no distinct $s_1, s_2, s_3 \in T_2$ and integers $i \neq j$ with $0 < |i|, |j| \leq L$ and $j(s_2 - s_1) = i(s_3 - s_1)$.

For $L = 2$ this excludes three-term progressions ($i = 1$, $j = 2$). Problem 5.1.4(ii) shows that it says more.

Problem 5.2.5. For $S = 3$, $D = 3$, $L = 2$, so $B = 24$, the sphere with the most points is $k = 5$, with the six permutations of $(0, 1, 2)$, and $T_2 = \{26, 49, 578, 624, 1153, 1176\}$.

It remains to choose S and D. Behrend lets S grow with n. For the density $x^{-\varepsilon}$ a fixed dimension suffices: let $S > 12/\varepsilon$ be a fixed integer and $D := \lfloor (n/4L)^{1/S}/(4L) \rfloor$.

Problem 5.2.6. (i) $B^S \leq n/(4L)$, so $4Ls < n$ for every $s \in T_2$. (ii) If $(n/4L)^{1/S} \geq 8L$, then $|T_2| \geq n^{1-2/S}(8L)^{-S}/S$.

Since $n^{-2/S} \geq (2x^{2+8\varepsilon})^{-\varepsilon/6} \geq x^{-\varepsilon/2}$ and $(8L)^{-S}/S \geq (8C_L \log x)^{-S}/S \geq x^{-\varepsilon/2}$ for large x, Problems 5.2.2–5.2.4 and 5.2.6 prove the following.

Theorem 5.2.1 (Behrend)**.** *For x large in terms of ε and C_L there is a set T_2 of nonnegative integers with $4Ls < n$ for $s \in T_2$, with $|T_2| \geq x^{-\varepsilon} n$, and with the property of Problem 5.2.4.*

Optimizing S gives the density $L^{-1} \exp(-C\sqrt{\log n \log L})$ [Adr, Prop. 5.17], which is Behrend's bound for $L = 2$ [Beh]. No construction can give a density bounded below: by Roth's theorem [Ro] a set of integers in $[0, n)$ without three-term progressions has $o(n)$ elements.

Now pass to $\mathbb{Z}/n\mathbb{Z}$. The condition $4Ls < n$ turns a congruence into an equation.

Problem 5.2.7. Let $u_0, t, h \in \mathbb{Z}/n\mathbb{Z}$ with h of order greater than $4L$. Among any L consecutive terms $t + ih$, at most two lie in $u_0 + T_2$.

Problem 5.2.8. If h has order at most $4L$, at most one element of $t + \mathbb{Z}h$ lies in $u_0 + T_2$.

Problem 5.2.7 uses only that h has order at least L; the threshold $4L$ is the one at which Problem 5.2.8 takes over. Problems 5.2.7 and 5.2.8 prove the following.

Theorem 5.2.2. *Let T_2 be as in Theorem 5.2.1, and $u_0, t, h \in \mathbb{Z}/n\mathbb{Z}$. If h has order greater than $4L$, at most two of any L consecutive terms $t + ih$ lie in $u_0 + T_2$. If h has order at most $4L$, at most one element of $t + \mathbb{Z}h$ does.*

So T_2 satisfies (1) and the second requirement of Section 5.1; for the cells this reads as follows.

Problem 5.2.9. Let p be as in Problem 5.1.2, and $u, t \in H$. If $2\iota_p$ has order greater than $4L$ in $\mathbb{Z}/n\mathbb{Z}$, then at most two of $\mathrm{cell}_t(p^{h_0}), \mathrm{cell}_t(p^{h_0+2}), \dots, \mathrm{cell}_t(p^{h_0+2L-2})$ are thick for w_u, for every odd $h_0 \geq 1$.

Theorems 5.2.1 and 5.2.2 are [Rub, Thm. III.3.1]. For $L(s, \psi)$ with ψ of order o, Section 4.5 requires $T_2 \subset A_0$. One applies the construction with n/o in place of n and places s at $s\,a_0$, with a_0 a generator of the cyclic group A_0 [Adr, §5].

5.3. The tops: a random choice

The set T of shifts t in Section 4.5, the *tops*, has the opposite needs. Its density $\delta_1 := x^{-\varepsilon/8}$ is larger, and along a Frobenius orbit it may contain a bounded number k_T of points in a window, not two. Exceptions are allowed if they are rare on average over primes. A random set does this, and this is where the argument uses randomness [Rub, §III.3], [Adr, Prop. 5.20]. Let $T \subset \mathbb{Z}/n\mathbb{Z}$ contain each element independently with probability δ_1.

Problem 5.3.1. $\mathbb{P}\big(\big||T| - \delta_1 n\big| > \frac{1}{2}\delta_1 n\big) \le 4/(\delta_1 n)$.

Problem 5.3.2. Let h have order at least L_2, and let W be a set of L_2 consecutive terms of $t + \mathbb{Z}h$. Then $\mathbb{P}(|W \cap T| \ge k_T + 1) \le (L_2\delta_1)^{k_T+1}$.

Problem 5.3.3. Let $k_T \ge 8(4 + 8\varepsilon)/\varepsilon$. If h has order at least L_2, the expected number of windows of L_2 consecutive terms on the orbits of h that contain more than k_T points of T is at most $2L_2^{k_T+1}x^{-2-\varepsilon/8}$.

With L_2 bounded and k_T as in Problem 5.3.3, a random T is thus sparse along the orbits of one h with probability close to 1. The argument asks for two more conditions of even spread along the orbits. It conditions on $t \in T$ and weights the primes by $\log p/p$, and it takes different probabilities on the cosets of A_0 to obtain the shares of Problem 4.5.3. Then it chooses one T by comparing expectations [Rub, Thm. III.3.2], [Adr, Prop. 5.20]. Compare Problem 5.1.5: the same method fails for T_2, where at most two points are allowed in a window and there may be no exceptions. For T_2 the sphere replaces chance. This ends the reduction: the Riemann hypothesis now asks for an upper bound for weighted prime sums at one scale, and the next part, from Chapter 6 on, gives the method that bounds them by comparing divisibility with size.

Exercises.

(1) Let $\log L \le c \log n$ with c small. With $S \approx \sqrt{\log n/\log L}$ and $D := \lfloor (n/4L)^{1/S}/(4L) \rfloor$, the construction gives $|T_2| \ge n\exp(-C\sqrt{\log n \log L})$, still with $4Ls < n$, for an absolute constant C.
(2) Without the condition $4Ls < n$, Problem 5.2.7 fails: for $n = 64$ and $L = 3$, the set $\{0, 2, 33\}$ has the property of Problem 5.2.4, yet $0, 33, 66 \equiv 2$ are consecutive terms of $33i$, of order 64.
(3) A set $T_2 \subset [0, n)$ with the property of Problem 5.2.4 meets every arithmetic progression of L terms in $\mathbb{Z}$ in at most two points.

Hints

§5.1.

5.1.1: By induction, $5^{2^e} \equiv 1 + 2^{e+2} \pmod{2^{e+3}}$; and -1 is not a power of 5 modulo 4.
5.1.2: Problem 4.1.3; $\chi_q(p^h) = \chi_q(p)$ for odd h.
5.1.3: Count the solutions u of $t[r] \in uT_2$.
5.1.4: (i) Add $a + c$ digit by digit.
5.1.5: The three points are distinct; count the h of order at most $4L$ in a cyclic group.
5.1.6: Linearity of expectation: $|R'|$ is at least $|R|$ minus the number of bad pairs.

§5.2.

5.2.1: Expand $|v_1 + b|^2 = |v_1|^2$ for $b = v_2 - v_1$ and for $c = v_3 - v_1$, and eliminate $v_1 \cdot c$.
5.2.2: Count the possible values of $|v|^2$.
5.2.3: Look at the lowest nonzero c_m modulo B.
5.2.4: Apply Problem 5.2.3 to the digits of $j(s_2 - s_1) - i(s_3 - s_1)$.
5.2.6: (ii) $\lfloor z \rfloor \geq z/2$ for $z \geq 1$, and Problem 5.2.2.
5.2.7: Eliminate h from three such terms, and bound the resulting integer.
5.2.8: If m is the order of h, then $m(s_1 - s_2) \equiv 0$.
5.2.9: Problems 5.1.2 and 5.2.7.

§5.3.

5.3.1: Chebyshev's inequality.
5.3.2: Union bound over subsets of W of size $k_T + 1$.
5.3.3: There are n windows.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[Beh] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U.S.A. **32** (1946), 331–332.

[Ro] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109.

[Rub] *The Alpöge–Claude proof of the Riemann hypothesis explained for the Riemann zeta function*, written by AI models at the behest of M. O. Rubinstein, working draft, 21 November 2026, `https://www.math.uwaterloo.ca/~mrubinst/alpoge_claude_grh/zeta-paper.pdf`.