A strict upper bound for restricted sparse rulers

18 November 2026

Abstract

We construct complete restricted sparse rulers of arbitrarily large span N with $125|A|^2 \leq 374N$. The construction assigns subspaces over a finite field to pairs of marks, then transfers their differences to an integer interval. A Lean 4 formalization proves the fixed bound $374/125 = 2.992$. Keeping the unrounded estimates gives an asymptotic upper bound of $2.9913220416\ldots$.

A *complete restricted ruler* of span N is a set $A \subseteq \{0, \ldots, N\}$ such that for each $1 \leq d \leq N$ there is an a with $a, a + d \in A$. Let $F(N)$ be its minimum possible cardinality. Brauer studied this restricted problem [4]. Answering a question of Rédei, Erdős and Gál proved that $c = \lim_{N\to\infty} F(N)/\sqrt{N}$ exists [7]. For unrestricted difference bases, Rédei and Rényi obtained a lower bound [19] that Leech sharpened [12] and Bernshteyn and Tait strictly improved [3]. These bounds on the squared asymptotic constant apply to c^2 as well, since allowing marks outside the interval can only reduce the minimum number of marks.

Following work of Haselgrove and Leech on restricted bases [9], Wichmann generalized Leech's ruler of span 36 to a family giving $c \leq \sqrt{3}$ [12, 24]. Miller gave a proof of completeness [15, App. A]. For extended Wichmann rulers we used the self-contained proof of Saarela and Vanhatalo [21, Thm. 18]. Luschny conjectured that, beyond thirteen segments, every complete ruler of greatest span for its number of marks is of Wichmann type up to reflection [13]. Pegg investigated this conjecture computationally [16]. It would imply $c = \sqrt{3}$, since Wichmann's length formula gives $3N \leq k^2 + k - 2$ for a ruler of this type with k marks.

Theorem 1. *For every $L \in \mathbb{N}$ there is an $N > L$ and a complete restricted ruler A of span N with $125|A|^2 \leq 374N$. In particular $F(N)^2/N$ cannot converge to 3.*

Write $[n] = \{0, \ldots, n-1\}$. We first allow marks in $[n] \times G$, where G is a finite abelian group. A target $(d, g) \in [n] \times G$ is measured if it is an ordered difference of marks in $\mathbb{Z} \times G$. For a set of marks S, write

$$\sigma = \frac{|S|}{\sqrt{n|G|}}, \qquad \delta = \frac{|\mathcal{E}|}{n|G|},$$

where $\mathcal{E}$ is a set of exceptional targets outside which coverage is guaranteed. For a prime q, we use $q + 1$ disjoint pairs for a target, each joining a baseline mark to a partner. Together the pairs supply every value of an additional group coordinate, and a partner needs only $1/q$ as many new labels as a baseline mark.

1 Simultaneous covers by hyperplanes

The $q + 1$ lines of $\mathbb{F}_q^2$ cover the plane [11]. Pulling these lines back along a surjective linear map gives a cover by hyperplanes. The lemma realizes one such cover for each prescribed matching, using the same subspace at a vertex wherever that vertex occurs.

Lemma 2. *Let q be prime and B, Y finite sets. For each member d of a finite nonempty set $\mathcal{D}$, let $M_d \subseteq B \times Y$ be a matching of size $q + 1$. Suppose that each pair belongs to at most one matching. There are a single $\mathbb{F}_q$-space V of dimension $2h$ and subspaces P_b, R_y of dimensions $h, h - 1$, respectively, such that*

$$P_b + P_{b'} = V \quad (b \neq b'), \qquad \bigcup_{(b,y)\in M_d} (P_b + R_y) = V \quad (d \in \mathcal{D}).$$

Proof. Put $F = \mathbb{F}_q$. Choose a finite extension E/F with $|E| > \max(|B|, q)$ and $\theta \in E \setminus F$. In E^2 the pairs $(1, 0)$ and $(\theta+t, 1)$, $t \in F$, represent the $q+1$ lines of the F-plane $\{(u+\theta v, v) : u, v \in F\}$. All have nonzero first coordinate and distinct slopes. At each d, assign these lines bijectively to the matched vertices b. Write $\lambda_{db} = z/w$ for the slope assigned via (w, z). Give all remaining b's distinct unused slopes, and reserve one further unused slope.

Let $U = E \times E^B$, $X = U^{\mathcal{D}}$, $W = X \times X$ and $V = W^\vee$, taking duals over F. Write $h = \dim_F X$. In W put

$$D_b = \{(x, (\lambda_{db} x_d)_{d \in \mathcal{D}}) : x \in X\}.$$

Each D_b has dimension h, and distinct D_b's intersect in zero. Their annihilators $P_b = D_b^\perp$ therefore satisfy the first assertion.

For a fixed y we specify an F-linear map $T_d : U \to U$ and a vector $e_d \neq 0$ in each block. If y is unmatched at d, let T_d multiply by the reserved slope and choose any $e_d \neq 0$. If y is matched to b, abbreviate λ_{di} to λ_i. Choose an F-linear functional $f : E \to F$ with $f(w) = 1$, for the assigned pair (w, z). Write $x = (x_*, (x_i)_{i \in B})$. Take e_d to have entry w in coordinate b and zero elsewhere, and set

$$(T_d x)_* = \lambda_b x_* + \sum_{i \in B} (x_i - x_*),$$

$$(T_d x)_i = \lambda_i x_i + \begin{cases} x_* - f(x_*) w & i = b, \\ (\lambda_b - \lambda_i) x_* & i \neq b. \end{cases}$$

Define $D'_y = \{(x, (T_d x_d + c e_d)_d) : x \in X,\ c \in F\}$ and $R_y = (D'_y)^\perp$. The first component determines x, and then any nonzero e_d determines c. Thus $\dim_F D'_y = h + 1$.

For $(b, y) \in M_d$, consider a vector in $D_b \cap D'_y$. At block d, the equation $T_d x + c e_d = \lambda_b x$ in coordinate b gives $x_* - f(x_*) w + c w = 0$. Applying f gives $c = 0$, so $x_* \in Fw$. The other coordinates force $x_i = x_*$, and the central coordinate then forces $x_b = x_*$ as well. At another block where y is matched to $b' \neq b$, the equation at coordinate b gives $(\lambda_{b'} - \lambda_b) x_* = 0$, using that block's slopes. All coordinates other than b are then zero, and the central equation forces $x_b = 0$. At unmatched blocks the distinct slopes force zero directly. The hypothesis on repeated pairs exhausts the possibilities.

Thus a vector in $D_b \cap D'_y$ vanishes outside d, and at d it is a multiple of the pair of constant vectors with entries w, z. Each such multiple satisfies the equations, giving the entire line. As (b, y) ranges over M_d, these lines exhaust a single two-dimensional plane. Every element of V vanishes on some line of that plane. Since $(D_b \cap D'_y)^\perp = P_b + R_y$, the second assertion follows. □

2 Finding the matchings

Choose primes $q \geq 10^{40}$ and $p \geq 10^{40} q^2$. Put

$$s = \lfloor p/4000 \rfloor + 1, \quad m = 1000s, \quad n = 12m, \quad \ell = q^2, \quad k = 4946sq.$$

In particular $p \leq 4m \leq p + 4000$ and $n \leq 6p$. The parabola $x \mapsto (x, x^2)$ is the finite-field form of the quadratic Sidon construction of Erdős and Turán [8, §I], described in these coordinates by Cilleruelo [5, §2.1]. Its differences cover $\mathbb{F}_p^\times \times \mathbb{F}_p$, as in Banakh and Gavrylkiv [2, Lem. 5.3]. We lift the parabola to integer heights from $4m$ to $12m - 1$ and add the full fiber at zero, giving the baseline marks in $[n] \times \mathbb{F}_p$

$$B = (\{0\} \times \mathbb{F}_p) \ \cup \ \{(j, j^2 \bmod p) : 4m \leq j < 12m\}.$$

Call a target $D = (d, a)$ interior if $d + \ell \leq n$ and $p \nmid d$. There are at most $(\ell + 6)p$ other targets. Every interior target is in $B - B$. For $d < 4m$, the lower indices $4m \leq j < 12m - d$ include a complete residue system, and the differences $2dj + d^2$ cover $\mathbb{F}_p$. For $d \geq 4m$ use the mark at d and one at zero.

2.1 Counting potential partners

The sampling weights depend only on height. At each position $(j, z) \in [n] \times \mathbb{F}_p$ place t_j tickets, where

$$t_j = \ell w_{\lfloor j/m \rfloor} + 2232m\,\mathbf{1}_{\{j<\ell\}}.$$

We found the weights by solving a linear program with HiGHS [10]. Multiplying the solution coordinates by 1000 and rounding up gives the twelve integers w_i below and the endpoint coefficient $558 = 2232/4$. The w_i sum to 2714, so the number of tickets is $T = 4946mp\ell$ and $k/T = q/(1000p\ell)$. A single position carries at most $R = 443\ell + 2232m \le 2000p$ tickets.

For an interior $D = (d, a)$, let H_D count tickets at positions y for which $b - y = D$ or $y - b = D$ for some $b \in B$. We claim

$$4002p\ell \le 4(H_D + 8R). \tag{1}$$

At height d all p tags qualify using baseline height zero. At any height j, a baseline parabola mark at $j + d$ supplies the tag $(j + d)^2 - a$, and one at $j - d$ supplies $(j - d)^2 + a$. Counting these contributions separately overcounts at most $8R$ tickets. At $j = d$ there are at most two extra tags. At every other height a coincidence requires $4jd = 2a \bmod p$. This singles out one residue of j, occurring at most six times in $[n]$.

To count before subtracting overlaps, write $d = im + r$, $0 \le r < m$. Set $b_j = \mathbf{1}_{\{4\le j<12\}}$ for all integers j and

$$S_e(i) = \sum_{j=0}^{11} w_j(b_{j+i+e} + b_{j-i-e}), \qquad e = 0, 1.$$

The height-zero baseline contributes at least $p\ell w_i$. If $b_i = 1$, every $0 \le j < \ell$ can use a parabola mark at $j + d$. Its extra tickets contribute $2232m\ell \ge 558p\ell$ in total. The remaining parabola contributions from the weights ℓw_j are exactly $\ell((m - r)S_0(i) + rS_1(i))$. Indeed shifting a bin of m consecutive heights by d puts $m - r$ sites in bin $j + i$ and r in bin $j + i + 1$. Shifting by $-d$ gives bins $j - i, j - i - 1$ in the same proportions. Since $p \le 4m$, it suffices for (1) that $4(w_i + 558b_i) + S_e(i) \ge 4002$ at both endpoints. The last row gives the smaller of the two values for each i.

i	0	1	2	3	4	5	6	7	8	9	10	11
w_i	298	312	312	323	0	0	22	132	213	291	368	443
Minimum	4010	4010	4009	4006	4601	4288	4008	4005	4006	4006	4002	4004

2.2 One sample for all targets

Draw k tickets independently and uniformly with replacement. For each interior D, fix one witnessing b at every eligible position. A draw at such a position is a hit assigned to b. The hit count Z has mean $\mu = kH_D/T$ and variance at most μ. Equation (1), $R \le 2000p$, and $\ell \ge 10^5$ give

$$\mu \;\ge\; q\left(\frac{4002}{4000} - \frac{16}{\ell}\right) \;\ge\; \frac{5001}{5000}\,q.$$

For a fixed b only the positions $b + D, b - D$ can supply a hit. If π_b is the probability of this assignment on one draw, then $k\pi_b \le 2Rk/T \le 4/q$.

Let Z_b count hits assigned to b, and let $C = \sum_b Z_b(Z_b - 1)$. There are at least $Z - C$ distinct assigned vertices, and independence gives $\mathbb{E}C = k(k - 1)\sum_b \pi_b^2 \le 4\mu/q$. With $\xi = \mu/10^5$ we have $q + 2\xi \le \mu$. If at most q distinct vertices occur, then $Z \le \mu - \xi$ or $C \ge \xi$. Chebyshev's and Markov's inequalities bound the probability of this event by

$$\frac{\mu}{\xi^2} + \frac{4\mu}{q\xi} \le \frac{10\,000\,400\,000}{q}. \tag{2}$$

Averaging over the common sample, choose a realization for which the fraction of all targets omitted (noninterior or failed) is at most

$$\frac{\ell+6}{n}+\frac{10\,000\,400\,000}{q}+\frac{1}{np}. \tag{3}$$

This is at most 10^{-20} for the chosen primes. At each remaining target choose $q+1$ distinct assigned vertices and one draw index per vertex. These indices are distinct, so they give a matching between B and the set Y of draw indices. An index retains its sampled position even if another draw landed there. A pair (b,y) determines at most one positive-height target, since the heights determine the order of subtraction.

2.3 Covering all labels at a good target

Apply Lemma 2 to the matchings. Enlarge the label group to $G=\mathbb{F}_p\times(\mathbb{Z}/2)\times V$. At each baseline mark put the additional coordinates $(0,P_b)$, and at each sampled position put $(1,R_y)$ for its draw index. At a good target two distinct baseline marks measure every even label, since $P_b-P_{b'}=V$. Cross pairs measure every odd label, since subtraction in either order gives the same subspace P_b+R_y. Thus (3) bounds δ after enlarging the group as well. There are at most $(p+8m)q^h+kq^{h-1}$ marks. It follows that

$$\sigma\le\frac{p+8m+k/q}{\sqrt{24mp}}\le\frac{8473}{2000\sqrt{6}}\sqrt{\frac{4m}{p}}\le 1.7296. \tag{4}$$

The last inequality uses $4m\le p+4000$. We have obtained a labeled set with $n\ge 10^{30}$, $\sigma\le 1.7296$, and $\delta\le 10^{-20}$.

3 Returning to the integer interval

Erdős and Gál [7, pp. 1156–1157] adapted a product method of Rédei and Rényi [19] to restricted rulers. They combined a coarse ruler S with a perfect cyclic difference set P of Singer [23] to form $vS+P$, using the two possible integer differences r and $r-v$ for a residue modulo v. Pikhurko and Schoen used this product to count the distinct differences of incomplete sets [18, proof of Thm. 3]. To fold a cyclic label into the height, we need r and $r+1$ to admit a common carry for almost every r.

Lemma 3. *For each $\eta>0$ there are arbitrarily large periods v and $P\subseteq[v]$ with $|P|\le(1+\eta)\sqrt{v}$ having the following property. For every $r\in[v]$ and bit e there is a bit c with $r+e-vc\in P-P$. For all but at most ηv values of r, the same c works for both $e=0,1$.*

Proof. We first need arbitrarily large b with a cyclic difference basis $S\subseteq\mathbb{Z}/b\mathbb{Z}$, meaning $S-S=\mathbb{Z}/b\mathbb{Z}$, of size $(1+o(1))\sqrt{b}$. Take $b=u(u-1)$ for a prime u. In Chinese remainder coordinates $\mathbb{Z}/(u-1)\times\mathbb{F}_u$, take Ruzsa's set $\{(i,g^i)\}$, where g is a primitive root [20, Thm. 4.4]. For $a,t\neq 0$, the difference (a,t) occurs because $g^j(g^a-1)=t$ has a solution. Complete the two coordinate axes as in Banakh and Gavrylkiv [1, Thm. 3.5] by adding a difference basis on each axis. For order h, the residues of $\{0,\dots,s-1\}\cup\{s,2s,\dots,s^2\}$ suffice for $s=\lceil\sqrt{h}\rceil$. Thus S has size $u+O(\sqrt{u})$.

Put $k_0=\lfloor b/4\rfloor$. For each $0\le r<k_0$ fix cyclic witnesses for r and $r+1$. For either witness the starting mark lies in the last k_0 sites in at most one of the three translations by $0,k_0,2k_0$, since the three positions are separated circularly by at least k_0. At least one translation puts both starting marks outside those last sites. In that translation neither difference wraps. By counting successful pairs of residues and translations, one translation works for at least $k_0/3\ge b/24$ residues when $b\ge 8$. Use that translate of S as integer digits in $[b]$.

Form P from all words of length a in these digits, with period $v = b^a$. Write $r = \sum_{i=0}^{a-1} r_i b^i$. Starting with $c_0 = e$, choose $c_{i+1} \in \{0, 1\}$ so that $r_i + c_i - bc_{i+1}$ is an ordinary digit difference. Cyclic coverage gives such a choice, including at $r_i + c_i = b$. Make the choice deterministic in (r_i, c_i), taking zero for either input at the successful residues above. The sum of the digit differences times b^i telescopes to $r + e - vc_a$. Any successful digit makes the two possible incoming carries agree from that point on. The exceptional fraction is at most $(23/24)^a$. Choose a to make it at most η, then take b sufficiently large that $(|S|/\sqrt{b})^a \le 1 + \eta$. □

Folding a cyclic coordinate. Suppose the current label group is $G' \times \mathbb{Z}/h\mathbb{Z}$, $h \ge 2$. Represent a mark as (i, g, t) with $0 \le t < h$ and replace it by

$$(h(vi + u) + t, g), \qquad u \in P.$$

The new height count is $n' = nvh$. For a target of height $h(vj + r) + s$, with $j < n - 1$, $r \in [v]$, $s \in [h]$, let $g \in G'$ be its remaining label. At a good r use the common carry c of Lemma 3. Request the old target $(j + c, g, s \bmod h)$. If a pair represents it, its two last-coordinate representatives differ by $s - he$ for some bit e. Choosing the fine difference $r + e - vc$ then gives exactly $h(vj + r) + s$.

For fixed good r the request is injective in (j, g, s). Thus old exceptions contribute at most their original fraction. The exceptional r's and the terminal band $j = n - 1$ contribute at most $\eta + 1/n$. The new normalized mark count is at most $(1 + \eta)\sigma$. For a finite product of cyclic groups, the length at least doubles at each fold, so all terminal losses sum to at most $2/n$. Choose the finitely many digit tolerances small enough that their sum and the total additive increase in normalized mark count are each at most ε. This removes all labels, giving an ordinary set in $[n']$, $n' \ge n$, with

$$\sigma' \le \sigma + \varepsilon, \qquad \delta' \le \delta + 2/n + \varepsilon. \tag{5}$$

The additive group of V is a product of cyclic groups of order q, so this applies to the group used in (4).

Filling the exceptional distances. Erdős and Gál placed a consecutive block and spaced marks at the ends [7, p. 1157, (5)].[1] We use one such block for all exceptional bands, including the terminal band. Suppose the resulting set $S' \subseteq [n']$ has H exceptional distances. Take $v > n'$ and P as in Lemma 3 with tolerance $\gamma > 0$. Place $vS' + P$ in $[n'v]$. A fine representative of $r \in [v]$ has ordinary value r or $r - v$. Thus all of the band $[tv, (t + 1)v)$ is measured if $t, t + 1$ are represented differences. Declare the terminal band and every band adjacent to an exceptional coarse difference bad. Their number J satisfies $1 \le J \le \min(n', 2H + 1)$.

Put $s_0 = \lfloor \sqrt{Jv} \rfloor + 1$ and add the common block $[s_0]$. Partition each bad band into intervals of at most s_0 consecutive integers and add their right endpoints. Subtracting the common block measures every point of each interval. All added marks lie in $[n'v]$, since $J \le n' < v$ implies $s_0 \le v$. They number at most $s_0 + J(\lfloor v/s_0 \rfloor + 1) \le 3s_0$, using $Jv < s_0^2$ and $J \le s_0$. Since $s_0^2 \le 4Jv$, the completed ruler A, of span $N = n'v - 1$, satisfies

$$\frac{|A|}{\sqrt{N + 1}} \le (1 + \gamma)\sigma' + 6\sqrt{2\delta' + 1/n'}. \tag{6}$$

Proof of Theorem 1. Use $\varepsilon = 10^{-22}$ in (5). Equations (3) and (4) give $\sigma' \le 1.72961$, $\delta' \le 10^{-18}$, $n' \ge 10^{30}$. With $\gamma = 10^{-6}$, the right-hand side of (6) is at most 1.7297. In particular

$$125|A|^2 \le 125(1.7297)^2(N + 1) \le 374N$$

for $N + 1 \ge 10^{30}$. The last period v can exceed any prescribed threshold. □

[1] With coarse span n, digit modulus v, and target span N, their product guarantees coverage through nv. The tail has length $N - nv$, one period more than the quantity $N - (n + 1)v$ used in their endpoint estimate.

Corollary 4 (Asymptotic refinement)**.** *There is a sequence of complete restricted rulers, with $N \to \infty$, for which*

$$\limsup \frac{|A|^2}{N} \le \frac{71\,791\,729}{24\,000\,000} = 2.9913220416\ldots.$$

Proof. Let $q \to \infty$ through primes and choose primes $p \ge \max(10^{40}q^2, q^4)$. Then $\ell/n \to 0$, $4m/p \to 1$, and the right-hand side of (3) tends to zero. Letting $\varepsilon, \gamma \to 0$ in (5) and (6) and using $(N+1)/N \to 1$ gives the square of $8473/(2000\sqrt{6})$ from (4). □

Computations and formalization. Preliminary finite searches used Luschny's ruler tables [13] and Pegg's sparse-ruler data [17]. SageMath [22] provided exact checks on small subspace examples and the rational weights. The accompanying proof of Theorem 1 uses Lean 4 [6] and the mathlib Community's library [14], both at version 4.24.0. Its theorem name is `SparseRulers.restricted_rulers_fixed_margin`.

References

[1] T. Banakh and V. Gavrylkiv. Difference bases in cyclic groups. *J. Algebra Appl.* **18** (2019), 1950081.

[2] T. Banakh and V. Gavrylkiv. Difference bases in finite Abelian groups. *Acta Sci. Math. (Szeged)* **85** (2019), 119–137.

[3] A. Bernshteyn and M. Tait. Improved lower bound for difference bases. *J. Number Theory* **205** (2019), 50–58.

[4] A. Brauer. A problem of additive number theory and its application in electrical engineering. *J. Elisha Mitchell Sci. Soc.* **61** (1945), 55–66.

[5] J. Cilleruelo. Combinatorial problems in finite fields and Sidon sets. *Combinatorica* **32** (2012), 497–511.

[6] L. de Moura and S. Ullrich. The Lean 4 theorem prover and programming language. *CADE-28*, LNCS **12699** (2021), 625–635.

[7] P. Erdős and I. S. Gál. On the representation of $1, 2, \ldots, N$ by differences. *Proc. Koninkl. Nederl. Akad. Wetensch.* **51** (1948), 1155–1158.

[8] P. Erdős and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* **16** (1941), 212–215.

[9] C. B. Haselgrove and J. Leech. Note on restricted difference bases. *J. London Math. Soc.* **32** (1957), 228–231.

[10] Q. Huangfu and J. A. J. Hall. Parallelizing the dual revised simplex method. *Math. Program. Comput.* **10** (2018), 119–142.

[11] A. Khare. Vector spaces as unions of proper subspaces. *Linear Algebra Appl.* **431** (2009), 1681–1686.

[12] J. Leech. On the representation of $1, 2, \ldots, n$ by differences. *J. London Math. Soc.* **31** (1956), 160–169.

[13] P. Luschny. Perfect and optimal rulers, section on the optimal ruler conjecture. *OEIS Wiki.*

[14] The mathlib Community. The Lean mathematical library. *Certified Programs and Proofs (CPP '20)*, ACM (2020), 367–381.

[15] J. C. P. Miller. Difference bases. Three problems in additive number theory. In *Computers in Number Theory*, Academic Press (1971), 299–322.

[16] E. Pegg Jr. Hitting all the marks: exploring new bounds for sparse rulers and a Wolfram Language proof. *Wolfram Blog* (2020).

[17] E. Pegg Jr. Sparse ruler data. *Wolfram Community* (2022).

[18] O. Pikhurko and T. Schoen. Integer sets having the maximum number of distinct differences. *Integers* **7** (2007), A11.

[19] L. Rédei and A. Rényi. On the representation of the numbers $1, 2, \ldots, N$ by means of differences (in Russian). *Mat. Sb. (N.S.)* **24(66)** (1949), 385–389.

[20] I. Z. Ruzsa. Solving a linear equation in a set of integers I. *Acta Arith.* **65** (1993), 259–282.

[21] A. Saarela and A. Vanhatalo. A connection between unbordered partial words and sparse rulers. *Electron. J. Combin.* **33** (2026), P1.40.

[22] The Sage Developers. SageMath, the Sage Mathematics Software System, version 10.10 (2026).

[23] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

[24] B. Wichmann. A note on restricted difference bases. *J. London Math. Soc.* **38** (1963), 465–466.