A famous packing problem—if you are not smart enough to count the dots then use applied probability

Phil. Howlett

E-mail: phil.howlett@unisa.edu.au

(with some help from Peter Pudney)

Scheduling and Control Group (SCG),
University of South Australia.

Three people that motivated my talk

Phil Pollett (the reason we are all here today at Uluru), Charles Pearce (who helped me to a deeper understanding of applied probability) and Jon Borwein (a legend who inspired my interest in convex analysis).

Problem description

Problem 1 Let $N \in \mathbb{N}$ be a natural number. For each subset $S \subseteq \mathbb{N}$ write $|S|$ to denote the number of elements in S. Consider all subsets $S \subseteq \{1, 2, \ldots, N\}$ that contain no 3-term arithmetic progression in the form $\{p - q, p, p + q\}$. What is the largest possible value for $|S|$? $\square$

This problem has not been solved. We will write $\nu(N)$ to denote the size of the largest subset of $\{1, 2, \ldots, N\}$ that contains no 3-term arithmetic progression.

George Szekeres (1911–2005)

George Szekeres received his degree in chemistry at the Technical University of Budapest. He moved to Shanghai prior to WWII to escape Nazi persecution of the Jews and later to Australia where he is now recognised as one of our greatest mathematicians.

The Szekeres conjecture

Conjecture 1 Let $N_r = (3^r + 1)/2$ where $r \in \mathbb{N}$. The largest subset $S_r \subseteq \{1, 2, \ldots, N_r\}$ which contains no three-term arithmetic progression has size $|S_r| = 2^r$. $\square$

This conjecture is false but when you look at the supporting evidence you may well be convinced (as I was at first) that it is true.

Supporting evidence for the Szekeres conjecture—a greedy algorithm

Write down the natural numbers in order but omit any terms that form a 3-term arithmetic progression. We find that

$$S_1 = \{1,2\}, \quad S_2 = \{1,2,4,5\}, \quad S_3 = \{1,2,4,5,10,11,13,14\},$$

$$S_4 = \{1,2,4,5,10,11,13,14,28,29,31,32,37,38,40,41\}, \ldots$$

which all looks so beautiful and convincing. Each set is symmetric so the greedy algorithm here is not blatantly biassed. If we write $A-B = \{a-b \mid a \in A,\ b \in B\}$ then $S_{r+1} = S_r \cup [\{(3^{r+1}+1)/2+1\} - S_r]$ for all $r \in \mathbb{N}$. The Szekeres sets show that

$$\nu((3^r+1)/2) \geq 2^r \quad \Rightarrow \quad \nu(N_r) \gg N_r^{1/\log_2 3}.$$

Supporting evidence for the Szekeres conjecture—the ternary expansion

Write down the non-negative integers in order using their ternary expansions but omit terms that contain a 2. Then add 1. We obtain

$$\{0, 1, [2], 10, 11, [12], [20], [21], [22], 100, 101, [102], 110, 111, \ldots\} + 1$$

which are the desired numbers. The powers (plus one) of the polynomials

$$p_1(z) = 1 + z, \quad p_4(z) = (1 + z)(1 + z^3),$$

$$p_{13}(z) = (1 + z)(1 + z^3)(1 + z^9), \ldots$$

also generate these numbers and all the roots lie on the unit circle.

It all seems so neat—but the Szekeres conjecture is false! What could possibly have gone wrong?

Felix Behrend (1911–1962)

Felix Behrend was another Jewish refugee. He fled Nazi Germany to Britain before WWII only to be detained in a Prisoner of War camp in 1940. He was later released following representations by influential mathematicians GH Hardy and JHC Whitehead but was transported to Australia and interred once again. He taught higher mathematics at *Camp University* to younger internees including future well-known mathematicians Walter F Freiberger, FI Mautner and JRM Radok. Textbooks were *not* provided but despite these difficulties the students were successfully prepared for exams at Melbourne University. Felix Behrend was released in 1942 and was subsequently appointed to a position at Melbourne University.

The Behrend construction—simple but elegant

Consider integers $d, n, k \in \mathbb{Z}$ with $d \geq 2$, $n \geq 2$ and $0 \leq k \leq n(d-1)^2$ and let $S_k(d,n) \subseteq \mathbb{Z}$ be the set of all numbers in the form

$$a = a_1 + a_2(2d-1) + a_3(2d-1)^2 + \cdots + a_n(2d-1)^{n-1}$$

where $a_i \in \mathbb{Z}$ with $0 \leq a_i \leq d-1$ for each $i = 1, 2, \ldots, n$ and such that

$$a_1^2 + a_2^2 + \cdots + a_n^2 = k.$$

For convenience we will also write

$$S = S(d,n) = \bigcup_k S_k(d,n).$$

The Behrend sets contain no arithmetic progressions

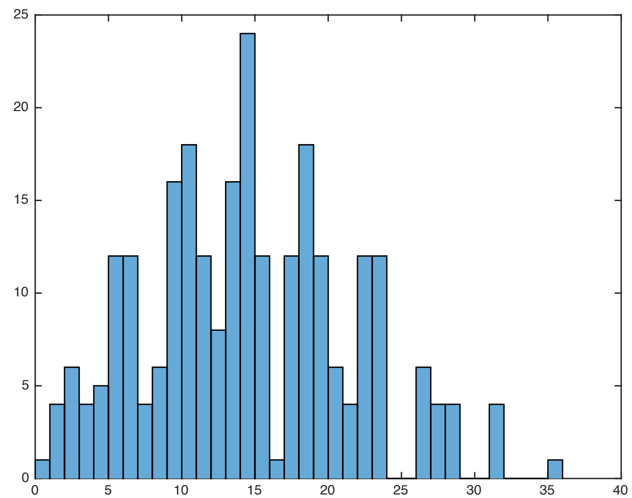
If we use base $2d-1$ to write the elements $a \in S$ in the form

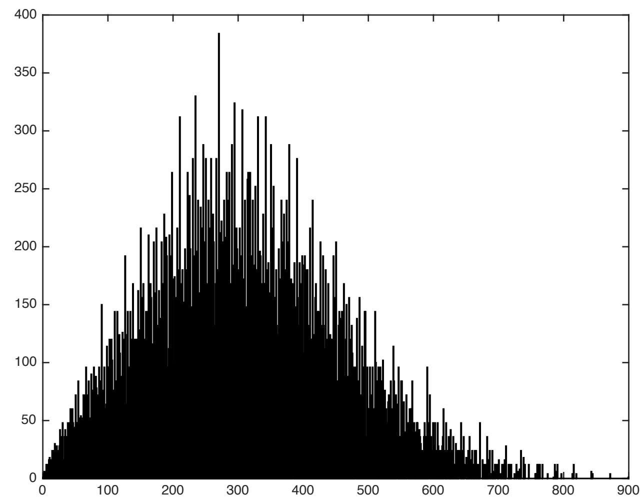
$$a = a_n a_{n-1} \cdots a_1$$

then the map $a \leftrightarrow \boldsymbol{v}(a)$ between $S \subseteq \mathbb{Z} \subseteq \mathbb{R}$ and $T \subseteq \mathbb{Z}^n \subseteq \mathbb{R}^n$ defined by $a_n a_{n-1} \cdots a_1 \leftrightarrow (a_1, a_2, \ldots, a_n)$ is a $1-1$ map. Because $0 \le a_i \le d-1$ and $0 \le b_i \le d-1$ the $1-1$ map extends to sums $a+b \leftrightarrow \boldsymbol{v}(a)+\boldsymbol{v}(b)$ and averages $(a+b)/2 \leftrightarrow (\boldsymbol{v}(a)+\boldsymbol{v}(b))/2$ provided $(\boldsymbol{v}(a)+\boldsymbol{v}(b))/2 \in \mathbb{Z}^n$.

If $a, b \in S_k(d,n)$ we say $\boldsymbol{v}(a), \boldsymbol{v}(b) \in T_k(d,n)$ and we note that $\boldsymbol{v}(a), \boldsymbol{v}(b)$ lie on the surface a sphere of radius $\sqrt{k}$. The convexity of the sphere means $(\boldsymbol{v}(a)+\boldsymbol{v}(b))/2$ lies in the interior and not on the surface. Thus $(\boldsymbol{v}(a)+\boldsymbol{v}(b))/2 \notin T_k(d,n)$. The $1-1$ map implies $(a+b)/2 \notin S_k(d,n)$.

Typical size distributions for the Behrend sets





Histograms for $|S_k(d,n)| = |T_k(d,n)|$ for $k \in [0, n(d-1)^2]$ in the cases $(d,n) = (4,4)$ with $k \in [0,36]$ on the left and $(d,n) = (16,4)$ with $k \in [0,900]$ on the right.

Applying the pigeonhole principle

There are d^n different vectors $\boldsymbol{v}(a) \in \{0, 1, \ldots, d-1\}^n$ but there are only $n(d-1)^2+1$ different values for k. Hence the pigeonhole principle means there is some $k = K$ with

$$|T_K(d,n)| \geq d^n/[n(d-1)^2+1].$$

Since $|S_K(d,n)| = |T_K(d,n)|$ and since all elements $a \in S_K(d,n)$ are less than $(2d-1)^n$ it follows that

$$\nu[(2d-1)^n] \geq d^n/[n(d-1)^2+1] > d^{n-2}/n.$$

The pigeonhole principle used here is our first encounter with applied probability. It just so happens that in this case the probability is one.

Estimating the lower bound

Let N be given. Choose $n = \lfloor \sqrt{2 \log_2 N} \rfloor$ and d so that $(2d-1)^n \leq N < (2d+1)^n$. Then

$$\nu(N) \geq \nu[(2d-1)^n] > d^{n-2}/n > N^{1-2/n}(1-N^{-1/n})^{n-2}/(n2^{n-2})$$

from which it follows that for N sufficiently large we have

$$\begin{aligned} \nu(N) &> N^{1-2/n}/(n2^{n-2}) \\ &= N^{1-2/n-\log_2 n/\log_2 N-(n-2)/\log_2 N} \\ &> N^{1-(2\sqrt{2}+\epsilon)/\sqrt{\log_2 N}} \end{aligned}$$

for any $\epsilon > 0$.

This is bigger than the Szekeres lower bound if $N > 2^{59}$. So it pays not to be greedy. The Behrend result was published in 1946 (in an easy-to-read 2-page paper) and remained the best result until 2008.

A new look at an old problem

Michael Elkin is a computer scientist and mathematician at Ben-Gurion University. Ben Green is a pure mathematician *extraordinaire* at the University of Oxford. Julia Wolf is a Reader in combinatorics and number theory at the University of Bristol.

Elkin's improved lower bound

We note that $N^{(2\sqrt{2}+\epsilon)/\sqrt{\log_2 N}} = 2^{\alpha}$ gives $\alpha = (2\sqrt{2}+\epsilon)\sqrt{\log_2 N}$. Thus Behrend's bound can be rewritten as

$$\nu(N) \gg N/2^{(2\sqrt{2}+\epsilon)\sqrt{\log_2 N}}.$$

By *careful analysis* of the Behrend sets Elkin used the principles of *applied probability* to find a marginally improved bound

$$\nu(N) \gg (1/\log_2 N)^{1/4} \cdot N/2^{2\sqrt{2}\sqrt{\log_2 N}}.$$

He then used a more elaborate analysis to find a further improvement

$$\nu(N) \gg (\log_2 N)^{1/4} \cdot N/2^{2\sqrt{2}\sqrt{\log_2 N}}.$$

We use a *brief note* by Green and Wolf to explain Elkin's bound.

It is a brief note—but I never said it would be easy

Imagine that d is really large but because we are so far away the hypercube $\{0, 1, \ldots, 2d-1\}^n$ looks like a unit n-cube composed of $N = (2d)^n$ uniformly distributed dots. Now we use *applied probability*.

Let $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ denote the n-dimensional torus and if $\boldsymbol{\theta}, \boldsymbol{\varphi} \in \mathbb{T}^n$ let $\Psi_{\boldsymbol{\theta},\boldsymbol{\varphi}} : \{1, 2, \ldots, N\} \to \mathbb{T}^n$ be the map defined by $p \mapsto p\,\boldsymbol{\theta} + \boldsymbol{\varphi} \pmod 1$.

Lemma 1 Fix $p, q \in \mathbb{N}$ with $p \neq q$. The variable $\Psi_{\boldsymbol{\theta},\boldsymbol{\varphi}}(p)$ is uniformly distributed on $\mathbb{T}^n$ and $(\Psi_{\boldsymbol{\theta},\boldsymbol{\varphi}}(p), \Psi_{\boldsymbol{\theta},\boldsymbol{\varphi}}(q))$ is uniformly distributed on $\mathbb{T}^n \times \mathbb{T}^n$ as $\boldsymbol{\theta}, \boldsymbol{\varphi}$ vary uniformly and independently over $\mathbb{T}^n$. $\square$

I know a little about two dimensional tori (doughnuts) but I know nothing about n-dimensional tori when $n > 2$. Do you? Anyway I decided to teach myself!

A concrete approach to high-dimensional tori (I)

Wikipedia says that the n-dimensional torus is the cartesian product of n circles. We should remember this.

When a circle is embedded in $\mathbb{R}^2$ the parametric equations are

$$x_1 = r_1 \cos 2\pi\theta_1, \; x_2 = r_1 \sin 2\pi\theta_1$$

where $r_1 > 0$ for $\theta_1 \in [0,1)$. This is $\mathbb{T}^1 \subseteq \mathbb{R}^2$. When a doughnut is embedded in $\mathbb{R}^3$ we can write the parametric equations in the form

$$x_1 = (r_1 + r_2 \cos 2\pi\theta_2) \cos 2\pi\theta_1,$$

$$x_2 = (r_1 + r_2 \cos 2\pi\theta_2) \sin 2\pi\theta_1, \; x_3 = r_2 \sin 2\pi\theta_2$$

where $r_1 > r_2 > 0$ for $\boldsymbol{\theta} = (\theta_1, \theta_2) \in [0,1)^2$. This is $\mathbb{T}^2 = \mathbb{T}^1 \times \mathbb{T}^1 \subseteq \mathbb{R}^3$.

Eureka! I can see a pattern emerging already.

A concrete approach to high-dimensional tori (II)

So I'm going to guess that the parametric equations for $\mathbb{T}^3 \subseteq \mathbb{R}^4$ are

$$
\begin{aligned}
x_1 &= (r_1 + (r_2 + r_3 \cos 2\pi\theta_3) \cos 2\pi\theta_2) \cos 2\pi\theta_1 \\
x_2 &= (r_1 + (r_2 + r_3 \cos 2\pi\theta_3) \cos 2\pi\theta_2) \sin 2\pi\theta_1 \\
x_3 &= (r_2 + r_3 \cos 2\pi\theta_3) \sin 2\pi\theta_2 \\
x_4 &= r_3 \sin 2\pi\theta_3
\end{aligned}
$$

where $r_1 > r_2 > r_3 > 0$ for $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3) \in [0,1)^3$; $\cdots$

A concrete approach to high-dimensional tori (III)

$\cdots$ and that for $\mathbb{T}^4 \subseteq \mathbb{R}^5$ the equations are

$$
\begin{aligned}
x_1 &= (r_1 + (r_2 + (r_3 + r_4 \cos 2\pi\theta_4) \cos 2\pi\theta_3) \cos 2\pi\theta_2) \cos 2\pi\theta_1 \\
x_2 &= (r_1 + (r_2 + (r_3 + r_4 \cos 2\pi\theta_4) \cos 2\pi\theta_3) \cos 2\pi\theta_2) \sin 2\pi\theta_1 \\
x_3 &= (r_2 + (r_3 + r_4 \cos 2\pi\theta_4) \cos 2\pi\theta_3) \sin 2\pi\theta_2 \\
x_4 &= (r_3 + r_4 \cos 2\pi\theta_4) \sin 2\pi\theta_3 \\
x_5 &= r_4 \sin 2\pi\theta_4
\end{aligned}
$$

where $r_1 > r_2 > r_3 > r_4 > 0$ for $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3, \theta_4) \in [0,1)^4$; $\cdots$

See—that didn't hurt too much did it! We needn't bother about higher dimensions because now it is dead easy. We need to be careful though—embedding $\mathbb{T}^n$ into $\mathbb{R}^{n+1}$ has everything to do with us and nothing much to do with the torus.

A concrete approach to high-dimensional tori (IV)

What about the $(n+1)$-surface area or more correctly the n-volume of $\mathbb{T}^n$? Well—if $\boldsymbol{x} = (x_1, \ldots x_{n+1})$ then the set $\partial \boldsymbol{x}/\partial\theta_1, \ldots, \partial\boldsymbol{x}/\partial\theta_n$ is an orthogonal set (you can check this from the parametric equations if you like or just hope it is—like me). Thus, for instance, we have

$$\begin{aligned}
V_3(\mathbb{T}^3) &= \int_{[0,1]^3} \left\|\frac{\partial \boldsymbol{x}}{\partial\theta_1}\right\| \left\|\frac{\partial \boldsymbol{x}}{\partial\theta_2}\right\| \left\|\frac{\partial \boldsymbol{x}}{\partial\theta_3}\right\| d\boldsymbol{\theta} \\
&= (2\pi)^3 \int_{[0,1]^3} [r_1 + (r_2 + r_3 \cos 2\pi\theta_3) \cos 2\pi\theta_2] \\
&\qquad\qquad [r_2 + r_3 \cos 2\pi\theta_3]\; r_3\, d\boldsymbol{\theta} \\
&= (2\pi)^3 r_1 r_2 r_3,
\end{aligned}$$

The $(2\pi)^3$ is just a scale factor. So we could say $V_3(\mathbb{T}^3) = r_1 r_2 r_3$. Come to think of it r_1, r_2 and r_3 are scale factors too. This n-torus is starting to *look* a bit like an n-cube.

A concrete approach to high-dimensional tori (V)

What have we achieved?

We know how to take cartesian products of circles; we know that $\mathbb{T}^n$ is an n-dimensional object; we understand the parametric equations that embed $\mathbb{T}^n$ into $\mathbb{R}^{n+1}$ and we know that the key gradient vectors defining the local curvilinear coordinates are mutually orthogonal; we can see that $\mathbb{T}^{m+n} \cong \mathbb{T}^m \times \mathbb{T}^n$; and we have also convinced ourselves that the volumes satisfy $V_{m+n}(\mathbb{T}^{m+n}) = V_m(\mathbb{T}^m) \times V_n(\mathbb{T}^n)$.

There's really not much else we need to know about tori. So now I'm hoping I don't have to explain Lemma 1.

The pigeonhole principle revisited

We identify $\mathbb{T}^n$ with $[0,1)^n$ in the obvious way. Let $\delta > 0$ be a suitably small fixed parameter. For each $r \leq n/4$ let

$$S_\delta(r) = \{\boldsymbol{x} \in [0,1/2]^n \mid r - \delta \leq \|\boldsymbol{x}\|^2 \leq r\}.$$

Lemma 2 For each $C > 1$ there exists some value $r = r_0 \leq n/4$ such that $V_n[S_\delta(r_0)] \geq c\,\delta 2^{-n}/\sqrt{n}$ where $c = 3\sqrt{5}(1 - 1/C^2)/C > 0$. $\square$

If $\boldsymbol{x} \in [0,1/2]^n$ is uniformly distributed the Chebyshev inequality gives

$$E\left[\left|\|\boldsymbol{x}\|^2 - n/12\right| \leq C \cdot \sqrt{n/180}\right] \geq 1 - 1/C^2.$$

Now probability is proportional to volume and we note that there are approximately $2C \cdot \sqrt{n/180} \cdot (1/\delta)$ sets $S_\delta(r)$ making up a total volume of $(1 - 1/C^2)2^{-n}$. The pigeonhole principle does the rest.

An application of the parallelogram law

Let $S_\delta = S_\delta(r_0)$. Suppose $\boldsymbol{x}-\boldsymbol{y}$, $\boldsymbol{x}$, $\boldsymbol{x}+\boldsymbol{y}$ all lie in S_δ. Since $2\|\boldsymbol{x}\|^2 + 2\|\boldsymbol{y}\|^2 = \|\boldsymbol{x}-\boldsymbol{y}\|^2 + \|\boldsymbol{x}+\boldsymbol{y}\|^2$ we must have $\|\boldsymbol{y}\|^2 \le \delta$. Thus $\boldsymbol{y} \in B_n(\sqrt{\delta}) \subseteq \mathbb{T}^n$ where $B_n = B_n(\sqrt{\delta})$ denotes the ball of radius $\sqrt{\delta}$. Stirling's approximation gives

$$V_n(B_n) = \pi^{n/2}\delta^{n/2}/\Gamma(n/2+1) \le (C\delta/n)^{n/2}$$

where $C = 2\pi e > 1$. Now $(\boldsymbol{x},\boldsymbol{y}) \in S_\delta \times B_n \subseteq \mathbb{T}^n \times \mathbb{T}^n$ and so

$$V_{2n}(S_\delta \times B_n) \le V_n(S_\delta)(C\delta/n)^{n/2}.$$

Ultimately the known constant $C = 2\pi e > 1$ obtained here will be used to define the constants in Lemma 2.

Using applied probability to count the dots

Lemma 3 Suppose $N \in \mathbb{N}$ is even. Define $A_{\boldsymbol{\theta},\boldsymbol{\varphi}} = \{p \in \{1,\ldots,N\} \mid \Psi_{\boldsymbol{\theta},\boldsymbol{\varphi}}(p) \in S_\delta\}$. Then the expected size of $A_{\boldsymbol{\theta},\boldsymbol{\varphi}}$ is

$$E_{\boldsymbol{\theta},\boldsymbol{\varphi}}\left[|A_{\boldsymbol{\theta},\boldsymbol{\varphi}}|\right] = N \cdot V_n(S_\delta)$$

and the expected number of 3-term arithmetic expressions in $A_{\boldsymbol{\theta},\boldsymbol{\varphi}}$ is

$$E_{\boldsymbol{\theta},\boldsymbol{\varphi}}\left[T(A_{\boldsymbol{\theta},\boldsymbol{\varphi}})\right] = N(N-2)/4 \cdot V_{2n}(S_\delta \times B_n).$$

□

Because the points are uniformly distributed the number of points in each set is proportional to the volume of the set. Counting the total number of 3-term arithmetic progressions is easy. For instance

$\{1,\ldots,8\} \supseteq \{123, 234, 345, 456, 567, 678; 135, 246, 357, 468; 147, 258\}.$

Completing the argument

If we choose $\delta = nN^{-2/n}/C$ then for sufficiently large N we have

$$V_n(S_\delta)/3 \geq (N-2)V_{2n}(S_\delta \times B_n)/4$$

from which it follows that

$$E_{\boldsymbol{\theta},\boldsymbol{\varphi}}\left[2|A_{\boldsymbol{\theta},\boldsymbol{\varphi}}|/3 - T(A_{\boldsymbol{\theta},\boldsymbol{\varphi}})\right] \geq NV_n(S_\delta)/3.$$

Hence there is at least one set $A = A_{\boldsymbol{\theta},\boldsymbol{\varphi}}$ such that $|A| \geq NV_n(S_\delta)/2$ and $T(A) \leq 2|A|/3$. This means we can remove all 3-term arithmetic progressions from A by deleting at most $2|A|/3$ elements. We are left with a set $A^{\#}$ for which

$$|A^{\#}| \geq NV_n(S_\delta)/6 = (c/6)\,\delta\,2^{-n}/\sqrt{n} = (c/6C)\sqrt{n}\,2^{-n}N^{1-2/n}.$$

When N is large we can maximize the right-hand side and obtain the desired bound by setting $n = \lfloor\sqrt{2\log_2 N}\rfloor$.

References

F. Behrend. *On sets of integers which contain no three terms in arithmetic progression*, Proc. Nat. Acad. Sci., **32**, 331–332, 1946.

M. Elkin. *An improved construction of progression-free sets*, available at http://arXiv:0801.4310v1 [math.NT] (20 pages), 2008.

B. Green and J. Wolf. *A note on Elkin's improvement of Behrend's construction*, available at http://arXiv:0810.0732v1 [math.CO] (4 pages), 2008.