Venn Symmetry and Prime Numbers: A Seductive Proof Revisited

Stan Wagon and Peter Webb

When he was an undergraduate at Swarthmore College in 1960, David W. Henderson [4] showed that there is a surprising connection between Venn diagrams and prime numbers

Theorem. If a symmetric n-Venn diagram exists, then n is prime.

An *n-Venn diagram* is a Venn diagram on n sets, which is defined to be a collection of n simple closed curves (Jordan curves) $C_1, C_2, \ldots, C_n$ in the plane such that any two intersect in finitely many points and each of the 2^n sets of the form $\bigcap C_i^{\epsilon_i}$ is nonempty and connected, where ϵ_i is one of "interior" or "exterior". Thus the Venn regions are all bounded except for the region exterior to all curves; each bounded region is the interior of a Jordan curve. See [6] for much more information on Venn diagrams. An n-Venn diagram is *symmetric* if each curve C_i is $\rho^i(C_1)$, where ρ is a rotation of order n about some center (we use O for the fixed point of rotation ρ).

We use Boolean notation for combinations of sets, with the 0-1 string $e_1\, e_2 \ldots e_n$ representing $\bigcap C_i^{\epsilon_i}$, where ϵ_i is interior (respectively, exterior) if $e_i = 1$ (respectively, 0). Thus 111 …1 represents F, the full intersection of all the interiors, 000 …0 is the intersection of all the exteriors (the unbounded region), and 100 …0 represents the set of points interior to C_1 and exterior to the others. In a symmetric Venn diagram, rotation of a region by ρ corresponds to a rightward cyclic shift of the Boolean string.

The universally familiar three-circle Venn diagram is symmetric, as is the one on two sets using two circles. For about 40 years a major open question was whether symmetric n-Venn diagrams exist for all prime n. Henderson found one for $n = 5$ and also (unpublished) for $n = 7$. Much later, Hamburger [3] settled the case of 11, which was quite complicated, and then in 2004 Griggs, Killian, and Savage [1] found an approach that works for all primes. So we now have the strikingly beautiful theorem that a symmetric n-Venn diagram exists if and only if n is prime.

But there is a small problem: Henderson's proof, which appears to be very simple, has a gap. Here is the proof from [4].

Suppose $1 \le k \le n - 1$. Since a symmetric n-Venn diagram is symmetric with respect to a rotation of $2\pi/n$, the regions corresponding to the Boolean strings with k 1s must come in groups of size n, each group consisting of one such region and its images under repeated rotation by $2\pi/n$. Therefore n divides $\binom{n}{k}$. This concludes the proof because the only n for which this is true for the specified k-values are the primes (an easy-to-prove fact of number theory; see [5]).

This is a very seductive argument. The primeness arises in such a cute way that one wants it to be true. Thus the proof has been repeated in many papers in the decades since it was first published. Yet there are problems. The proof does not call upon the connectedness of the Venn regions. Without connectedness the result is false; see Figure 1 (due to Grünbaum [2]), which shows a diagram satisfying all of the conditions for a symmetric 4-Venn diagram, except the one saying that the Venn regions must be connected. Note that this diagram has disconnected regions (for example, the region consisting of the two black triangles).

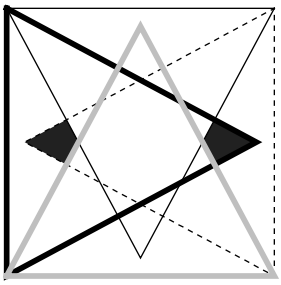

Figure 1. Rotating an equilateral triangle leads to a symmetric diagram that represents all 16 combinations of the four sets. But the set that represents a combination is not necessarily connected (as in the shaded case).

More important, the reasoning in Henderson's proof that the Venn regions come in groups of size n is insufficient, since it could perhaps happen that a Venn region R coincides with one of its rotated copies, thus disrupting the count. Certainly R cannot equal $\rho(R)$ (unless R is the common exterior or interior), because the Boolean string for R must include both a 1 and a 0 and therefore a cyclic shift of the string one place yields a different string, and therefore a region disjoint from R. However, some patterns are invariant under two rotations: the string 1010 is unchanged by two rightward shifts. This phenomenon would invalidate the proof, so to fix it one must show that in a symmetric n-Venn diagram, $\rho^i(R)$ cannot equal R if $1 \le i \le n-1$, unless R is either the common exterior or interior.

In email exchanges with Branko Grünbaum and David Henderson, alternative approaches to ours were proposed. These involved the use of winding numbers or similar ideas, all of which require that the curves in the Venn diagram be rectifiable. One can in fact reduce the general case to the rectifiable case, or even to the case that all curves are piecewise linear, but this adds the complexity of a compactness argument. Our approach — based on the following lemma — is self-contained and provides a purely geometric proof of a geometric fact. The lemma can be used either to fix Henderson's proof or to create a more direct proof with no reference to number theory. We require the Jordan curve theorem: every simple closed curve J in the plane divides the complement of J into two connected open sets, with J being the boundary of each.

Lemma. Let J be a simple closed curve invariant under a nonidentity rotation ρ about center O. Then O is in the interior of J.

Postponing the proof for a moment, we show how the theorem follows.

Proof of Theorem. Suppose the assertion is false, so that there is a composite number n with proper divisor b and a Jordan curve C such that, for a rotation ρ of order n, the curves $\rho^k(C)$, $k = 0, \ldots, n-1$, form an n-Venn diagram. Let R be the region with Boolean representation 100 100 … 100, with b bits in each block (here $b = 3$). Then both R and $\rho(R)$ are invariant under ρ^b and so the lemma places O in each of them. This is a contradiction because the two sets are distinct Venn regions (the Boolean representation of $\rho(R)$ begins with 01). □

And now the proof of the lemma:

Proof of Lemma. Let S be the exterior of J. Let x be a point on J that is farthest from O and let C denote the circle centered at O and passing through x; therefore J is contained in C and its interior. Note that J travels from x to $\rho(x)$ and then back to x, thus splitting into two paths, which we call J_1 and J_2. Suppose O is not in the interior of J. Then either $O \in S$ or O is on J. In the first case, let $z = O$. In the second case, when O is on J — on J_1, say — there is a small disk D about O that is inside C and disjoint from J_2. Such

a disk must contain a point $z \in S$. In either case, there is an unbounded path that starts at z and is contained in S. Let P be the truncation of such a path as soon as it reaches circle C, so that P goes from z to a point y on C and in S.

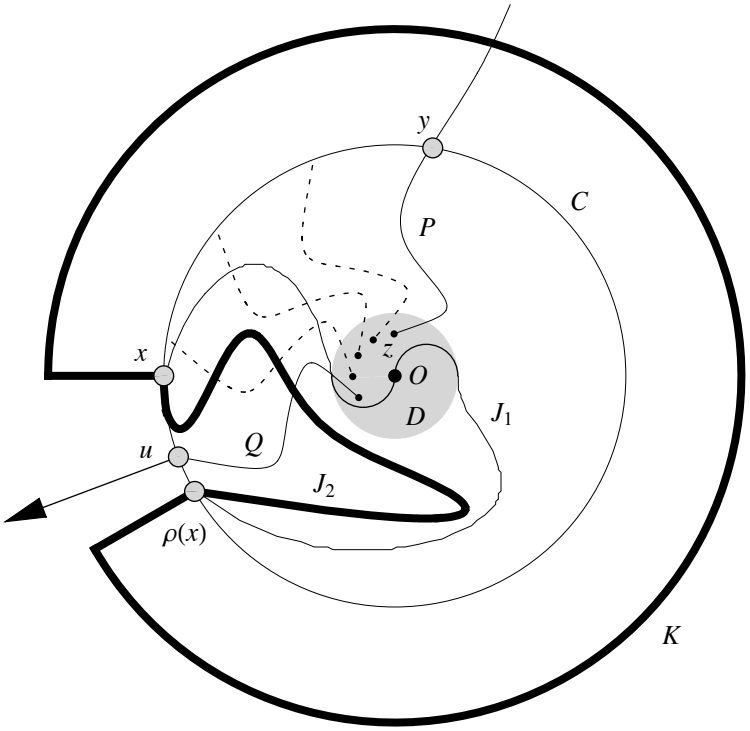

Figure 2. A schematic representation of the situation where O is on J. The point z is in the exterior of J and near O. Then one forms a path P from z to C and rotates the path to a path Q that connects the interior of K to its exterior.

Let B be a circle with center O and radius larger than that of C. Form the simple closed curve K that starts at x, follows path J_2 to $\rho(x)$, goes radially outward to B, follows an arc of B to the point radially aligned with x, and then goes radially inward to x. Of the two possible B-arcs, use the one that places z, indeed all of D, in the interior of K. The use of the larger circle guarantees that K's return trip to x misses J. Using the fact that y, being in S, cannot rotate to a point on J, we can rotate path P to $\rho^i(P) = Q$ so that y moves to u, a point on C whose radial extension to infinity does not intersect K (Figure 2). Symmetry implies that Q is contained in S. Because $\rho^i(z)$ is in disk D, it lies in the interior of K. But u is in the exterior of K. Thus Q connects the interior of K to its exterior, which means that Q intersects K, a contradiction as a common point would be on or inside C and so would be both in S and on J. □

Note the following useful consequence of the lemma: in a symmetric Venn diagram, O lies in F, the full intersection region. This is because F, and therefore its bounding curve, are invariant under the rotation. This sheds light on Henderson's proof as follows. Let R be a Venn region as in that proof. Then if $1 \le k \le n - 1$, it cannot happen that $\rho^k(R) = R$ because the lemma, applied to the boundary of R and the rotation ρ^k, would place O in the interior of R. Since O is also inside F, this is a contradiction. Therefore n does indeed divide $\binom{n}{k}$ whenever $1 \le k \le n - 1$, as claimed.

References

[1] J. Griggs, C. E. Killian, and C. D. Savage, Venn diagrams and symmetric chain decompositions in the Boolean lattice, *Electron. J. Combin.* **11** (2004) #R2.

[2] B. Grünbaum, Venn diagrams and independent families of sets, *Math. Mag.* **48** (1975) 12-23.

[3] P. Hamburger, Doodles and doilies, non-simple symmetric Venn diagrams, *Disc. Math.* **257** (2002) 423-439.

[4] D. W. Henderson, Venn diagrams for more than four classes, this MONTHLY **70** (1963) 424-426.

[5] F. Ruskey, C. Savage, and S. Wagon, The search for simple symmetric Venn diagrams, *Notices Amer. Math. Soc.* **53** (2006) 1304-1312.

[6] F. Ruskey and M. Weston, A survey of Venn diagrams, *Electron. J. Combin.* **4** (1997; revised 2005) DS5.

Department of Mathematics and Computer Science, Macalester College, St. Paul, MN 55105
wagon@macalester.edu

School of Mathematics, University of Minnesota, Minneapolis, MN 55455 webb@math.umn.edu