A formal proof of Pick's theorem
(extended abstract)

John Harrison

Intel Corporation, JF1-13
2111 NE 25th Avenue, Hillsboro OR 97124, USA
johnh@ichips.intel.com

Given a polygon with vertices at integer lattice points (i.e. where both x and y coordinates are integers), Pick's theorem [4] relates its area A to the number of integer lattice points I in its interior and the number B on its boundary:

$$A = I + B/2 - 1$$

We describe a formal proof of this theorem using the HOL Light theorem prover [2]. As sometimes happens for highly geometrical proofs, the formalization turned out to be quite challenging. In this case, the principal difficulties were connected with the triangulation of an arbitrary polygon, where a simple informal proof took a great deal of work to formalize.

Elementary triangle

We start by establishing the result for an *elementary* triangle: one whose vertices are lattice points and which contains no other lattice points either in its interior or boundary. Pick's theorem for such a triangle simply asserts that it has area $1/2$, or 0 in the degenerate cases where it is flat.

Given two vectors A and B, we can consider them as defining the linear transformation of the plane $f : (x, y) \mapsto Ax + By$. It is not hard to show that if the image under f of the set of integer lattice points is exactly this same set of integer lattice points, then the determinant of the matrix of f is ± 1:

```
|- ∀f:real^N->real^N.
        linear f ∧ IMAGE f integral_vector = integral_vector
        ⇒ abs(det(matrix f)) = &1
```

Given an elementary triangle OAB, where we take O as the origin, one can show that the integer multiples of the two other vertices generate precisely the integer lattice points. The determinant in the previous theorem is precisely twice the area of the triangle formed by the three vertices, which therefore has area $1/2$:

```
|- ∀a b c:real^2.
        {x | x IN convex hull {a,b,c} ∧ integral_vector x} = {a,b,c}
        ⇒ measure(convex hull {a,b,c}) =
              if collinear {a,b,c} then &0 else &1 / &2
```

Arbitrary triangle

Next, we proceed inductively to establish the result for an arbitrary triangle with all its vertices at integer lattice points. If a triangle ABC is not elementary, then it must have a lattice point D either:

- On one if its sides, say AB, in which case we can subdivide it into triangle ADC and BCD.
- In its interior, in which case we can divide it into three triangles ADB, ADC and BDC.

Although this is straightforward enough, we can make it even simpler, by reformulating things slightly so that the first case becomes a degenerate case of the second, and we avoid handling degenerate cases of the theorem itself separately. By a general result on additivity of a function defined on a set of lattice points, we deduce the following variant of Pick's theorem for a triangle. It is straightforward to show it equivalent to the usual formulation with a proviso of nondegeneracy.

```
|- ∀a b c:real^2.
    integral_vector a ∧ integral_vector b ∧ integral_vector c
    ⇒ measure(convex hull {a,b,c}) =
         &(CARD {x | x IN convex hull {a,b,c} ∧ integral_vector x}) -
         (&(CARD {x | x IN convex hull {b,c} ∧ integral_vector x}) +
          &(CARD {x | x IN convex hull {a,c} ∧ integral_vector x}) +
          &(CARD {x | x IN convex hull {a,b} ∧ integral_vector x})) / &2 +
         &1 / &2
```

Arbitrary polygon

Again, we proceed inductively, showing that any polygon can be subdivided into two by a line joining two vertices and otherwise lying entirely in the interior. (This can also be used to drive an inductive proof that any polygon can be triangulated, and that is where we looked for a proof, though we don't explicitly deduce this general result.) The informal proof, essentially excerpted from [1], seems relatively straightforward:

> Pick the coordinate axis so that no two vertices have the same y coordinate. Let B be the lowest vertex on the polygon, and let A and C be adjacent to B. If AC is an interior diagonal, we draw the diagonal AC, forming a triangle ABC and a polygon without the vertex C. Otherwise, let D be a vertex of the polygon at maximal distance from the line AC in the direction of B. Cut the polygon into two along the edge BD.

The first challenge is to formalize the 'pick the coordinate axis' step. An earlier paper [3] described an extensive framework for such 'without loss of generality' reasoning, but to support the present proof, this had to be generalized from 'first order' concepts like points and lines to 'higher order' concepts like polygonal paths and sets of points.

The next difficulty is to formalize the general notion of being 'inside' and 'outside' a polygon. In fact, we define this concept for a general closed curve, and use the Jordan curve theorem to deduce some of its important properties. For example, if one chops the inside of a closed curve in two with an arc across it, the inside divides into two in a fairly obvious way, and we use this to drive the main induction. But the proof of this in the general setting of simple closed curves turned out to be far from obvious; we formalized a 14-line proof from [5] (1.4, page 31), giving rise to a laborious 788-line formal counterpart.

Finally, we can follow through the informal proof. However, even this turned out to be quite difficult. One needs to work quite hard to establish that certain points lie 'inside' or 'outside' the polygon; we exploit a 'parity lemma' precisely characterizing how the inside/outside status switches as a line segment crosses segments of the polygon. It is also necessary to translate several completely obvious geometric arguments to do with orientation into tedious pieces of vector algebra. But finally, we obtain the overall result:

```
|- (∀x. MEM x p ⇒ integral_vector x) ∧
   simple_path(polygonal_path p) ∧
   pathfinish(polygonal_path p) = pathstart(polygonal_path p)
   ⇒ measure(inside(path_image(polygonal_path p))) =
       &(CARD
        {x | x IN inside(path_image(polygonal_path p)) ∧ integral_vector x}) +
       &(CARD
        {x | x IN path_image(polygonal_path p) ∧ integral_vector x}) / &2 -
       &1
```

References

1. T. C. Hales. Easy pieces in geometry. Available at `http://www.math.pitt.edu/~thales/papers/`, 2007.
2. J. Harrison. HOL Light: A tutorial introduction. In M. Srivas and A. Camilleri, editors, *Proceedings of the First International Conference on Formal Methods in Computer-Aided Design (FMCAD'96)*, volume 1166 of *Lecture Notes in Computer Science*, pages 265–269. Springer-Verlag, 1996.
3. J. Harrison. Without loss of generality. In S. Berghofer, T. Nipkow, C. Urban, and M. Wenzel, editors, *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2009*, volume 5674 of *Lecture Notes in Computer Science*, pages 43–59, Munich, Germany, 2009. Springer-Verlag.
4. G. Pick. Geometrisches zur Zahlenlehre. *Sitzungsberichte des deutschen naturwissenschaftlich-medicinischen Vereines für Böhmen "Lotos" in Prag, Series 2*, 19:311–319, 1899.
5. G. T. Whyburn. *Topological Analysis*, volume 23 of *Princeton Mathematical Series*. Princeton University Press, revised edition, 1964.