A Matroid-Quantum Connection

With tighter links between notions of rank?

James Oxley and Geoff Whittle are mathematicians at LSU and Victoria University (Wellington, New Zealand), respectively. They have written many joint papers on matroid theory, but none on quantum computing.

Today we observe that they really have *indirectly* written a paper on quantum computing.

Their paper, "A Characterization of Tutte Invariants of 2-Polymatroids," has implications for quantum complexity theory. It introduced a polynomial $S_G(x, y)$ where G is a graph and x, y are numbers. Like many polynomials defined on graphs this one is in general hard to compute—it is #P-hard, so if it is polynomial time computable, then surprising stuff happens.

The same paper observes that $S_G(x, y)$ is easy to compute when

uv = 1 for rational u, v.

However, a 2006 paper by Steve Noble proves that *all* other rational cases are #P-hard. Our work finds easy cases in another family where $v = \pm \sqrt{2}i$ and u is a rational multiple of $\sqrt{2}i$. This result goes through quantum complexity theory.

It is interesting to note that quantum computations welcome complex numbers such as $\sqrt{2}i$. In mathematics insights to behavior of real functions are often found when we extend them to the complex functions. A beautiful example to compare is that the behavior of

$$f(x) = \frac{1}{1+x^2}$$

is best understood by noting that $1 + x^2$ can be zero at x = i.

Matroids and Polymatroids

In order to best understand the above results it is helpful to look at matroids and generalizations. Matroids are a bit scary, since they seem quite abstract. But that is wrong. The matroid concept is a natural generalization of the notion of rank in an ordinary vector space.

Let's take a look. A *matroid* is defined by a set U and a function f from finite subsets of U to \mathbb{N} that obeys the following rules:

1.
$$f(\emptyset) = 0;$$

- 2. for all $a \in U$, $f(\{a\}) \le 1$;
- 3. if $A \subseteq B$ then $f(A) \leq f(B)$; and
- 4. if $A \subseteq B$ and $c \notin B$ then $f(A \cup \{c\}) f(A) \ge f(B \cup \{c\}) f(B)$.

The notion of rank in an ordinary vector space obeys these axioms. The rules are:

- 1. The empty set has rank 0;
- 2. Each vector has rank at most 1;
- 3. The rank of a set of vectors can increase only by adding more vectors;
- 4. Suppose that adding c to a set B increases the rank. Then c also increases the rank of any subset of B. Or if c is independent of a set of vectors B, then it is independent of any subset of B.

The definition of a *polymatroid* simply wipes out rule 2. OK, a k-polymatroid replaces it by the rule that for all singleton sets $\{a\}$ have $f(\{a\}) \leq k$. An important kind of 2-polymatroid springs from the following idea:

The "f-rank" of a subset A of the **edges** in a graph G is the number of vertices collectively touched by edges in A.

In a simple undirected graph, every edge has f-rank 2. In graphs with self-loops, however, the loops have rank 1. We can also allow the universe U to include members of f-rank 0. Those are visualized as loops without a vertex and called *circles*. We could also visualize edges of rank 1 that stick out from a vertex v into empty space, but those are formally the same as loops at v. This defines a graphic(al) 2-polymatroid M = (U, f).

The theory of polymatroids ignores the notion of "vertex" apart from the definition of the rank function f. Hence all graphs composed of m isolated vertices define the empty 2-polymatroid. To preserve the distinction, we define an m-graph to be a graph with circles allowed. The empty m-graph is denoted by \oslash and called a "wisp." Every m-graph specializes to a unique graphical polymatroid but we can include isolated nodes when thinking of it as a graph (plus circles).

Explosion and Contraction Again

We revisit the definition of "exploding" an edge e = (u, v) in a graph G from the previous post in this series:

- If there are an odd number of edges incident only to *u* and/or *v*, then *u* and *v* become a circle and a wisp, else they become two wisps.
- Any other edge incident to *u* or *v* from another vertex *t* becomes a loop at *t*.

If we ignore vertices, then the rank function f' of the resulting mgraph G' is such that for all subsets A' of its edge set $E' = E \setminus \{e\}$,

(1)
$$f'(A) = f(A \cup \{e\}) - f(\{e\}).$$

One can verify that the "explosion" description obeys (1). Glancing at our picture helps—we have varied the one in the previous post by showing how a loop at one exploded node becomes a circle:



The equation (1), however, is more fundamentally natural. The simple extension

$$f'(A) = f(A \cup T) - f(T)$$

defines the matroid contraction by any subset T of E. When $T = \{e\}$, it supersedes the graph-theory notion of contraction G/e in matroid contexts. Since we are talking about both, we will write $G \setminus e$ for the matroid version. The \setminus notation conveys that the edge e gets deleted emphatically.

The Polynomial $Q_G(x)$

In a previous post we derived a recurrence for the *amplitude* a(G) in terms of explosion. The presence of circles and use of the function f(e) now allows us to write it as:

$$a(G) = a(G \setminus e) - \frac{1}{f(e)}a(G \setminus e).$$

We can omit the " $(-1)^r$ " from the previous version because the circles keep track of this. The rule is valid even when e is a self-loop, using f(e) = 1. The following is thus a complete basis:

- For a wisp \oslash or isolated node •, $a(\oslash) = a(\bullet) = 1$.
- For a circle \bigcirc , $a(\bigcirc) = -1$.
- If G is the disjoint union of G_1 and G_2 , then $a(G) = a(G_1)a(G_2)$.

To get more mileage out of this, we want to emulate William Tutte's idea and define a polynomial $Q_G(x)$ whose evaluation at x = 1 gives a(G), and whose other evaluations may give more information. Without further ado:

Definition 0.1. For an m-graph G, define its **amplitude polynomial** $Q_G(x)$ inductively by:

- Q_G(x) = (−1)^kx^ℓ, if G consists of ℓ isolated nodes, k circles, and any number of wisps.
- For any edge e,

(2)
$$Q_G(x) = Q_{G\setminus e} - \frac{1}{f(e)} Q_{G\setminus e}.$$

Recall f(e) = 1 if e is a loop, else f(e) = 2. When G consists of a single node with a loop, the recursion gives $Q_{loop} = x - 1$. When it is a single edge e between two nodes, we get $Q_e(x) = x^2 - \frac{1}{2}$.

If we have a single node v with two loops, something portentous happens. Exploding one of the loops e leaves a circle. Removing e still leaves one loop. So we get:

$$Q_G(x) = Q_{loop}(x) - Q_{\bigcirc}(x) = x - 1 - (-1) = x.$$

This agrees with the value on one isolated node. Similarly, if G has just a double edge between two nodes u and v, then one edge

e becomes a circle upon exploding the other edge, so recursing on the other edge makes

$$Q_G(x) = Q_e(x) - \frac{1}{2}Q_{\bigcirc} = x^2 - \frac{1}{2} + \frac{1}{2} = x^2.$$

Thus the double edge gives the same result as having two isolated nodes. The upshot is that equation (2) naturally treats edges modulo two. We can recurse on a *non*-edge as if it were a double-edge, and the circle left by the explosion (i.e., by the matroid contraction) becomes a -1 multiplier on the entire remainder of that branch of the recursion. The *circle* thus becomes a placeholder for calculating phase flips and cancellations, which is why we believe the matroid notions are useful in analyzing quantum processes.

It may not be obvious, however, that $Q_G(x)$ is well-defined when G has more than one edge. That is, does it come out the same for any order of choosing edges e for the recursion? We will prove this by connecting Q_G to the polynomial $S_G(u, v)$ mentioned above.

Relation to the Rank-Generating Function $S_G(x, y)$

The original non-recursive definition of the rank-generating function of a graphical 2-polymatroid G = (E, f) is:

(3)
$$S_G(u,v) = \sum_{A \subseteq E} u^{f(E) - f(A)} v^{2|A| - f(A)}.$$

We compute some basic cases:

- 1. For the empty graph \oslash , or any graph G with only isolated nodes, we have only the term $A = E = \emptyset$, so $S_G(u, v) = 1$.
- 2. For a circle \bigcirc , we still have $f(\bigcirc) = 0$ even though $E \neq \emptyset$. The term $A = \emptyset$ still gives 1, but A = E now gives $u^{0-0}v^{2-0} = v^2$. Thus $S_\bigcirc(u,v) = 1 + v^2$.
- 3. For the graph G consisting loop at a single node, we have f(E) = 1, so the term for $A = \emptyset$ becomes $u^{1-0}v^{0-0} = u$. And the term for A = E is $u^{1-1}v^{2-1} = v$. So $S_G(u, v) = u + v$.
- 4. For G with a single edge between two nodes, $S_G(u,v) = u^{2-0}v^{0-0} + u^{2-2}v^{2-2} = u^2 + 1.$

Note the symmetry in u and v between cases 2 and 4 in particular, which could be brought out more by discussing how (graphical

poly-)matroids foster higher notions of *duality* than graphs do. Our theorem breaks this symmetry, but perhaps there is a deeper underlying law that would restore it:

Theorem 0.2. For any m-graph G with n nodes, of which k are isolated, and all $x \in \mathbb{C}$, taking $\alpha = -\sqrt{2}i$,

(4)
$$Q_G(x) = \left(\frac{1}{\alpha}\right)^n S_G(\alpha x, -\alpha)(\alpha x)^k.$$

Proof. Call $R_G(x)$ the right-hand side of (4). Note first that if G consists only of ℓ isolated nodes then $S_G(\cdot, \cdot) = 1$ so the right-hand side becomes

$$\left(\frac{1}{\alpha}\right)^{\ell} (\alpha x)^{\ell} = x^{\ell} = Q_G(x).$$

Now we verify the other base cases:

- 1. $R_{\otimes}(x) = (1/alpha)^0 \cdot 1 \cdot (\alpha x)^0 = 1 = Q_{\otimes}(x).$
- 2. $R_{\bigcirc} = 1 \cdot (1 + (-\alpha)^2) \cdot 1 = 1 2 = -1 = Q_{\bigcirc}(x).$
- 3. $R_{loop} = \frac{1}{\alpha}(\alpha x \alpha) = x 1 = Q_{loop}(x).$
- 4. For *G* with a single edge between two nodes, $R_G(x) = (\frac{1}{\alpha}^2)((\alpha x)^2 + 1) = x^2 + \frac{1}{\alpha^2} = x^2 \frac{1}{2} = Q_G(x).$

To verify the recursion, we note facts observed by Oxley and Whittle as consequences of (3):

(a) If e is a loop at a vertex with other incident edges, so f(e) = 1and $f(E \setminus \{e\}) = f(E)$, then

$$S_G(u, v) = S_{G \setminus e}(u, v) + v S_{G \setminus e}(u, v).$$

(b) If e is a pendant edge, i.e., between a node of degree 1 and a node of larger degree, so f(e) = 2 and f(E \ {e}) = f(E) − 1, then

$$S_G(u, v) = u S_{G \setminus e}(u, v) + S_{G \setminus e}(u, v).$$

(c) If e is an edge between nodes of degree at least 2, so f(e) = 2and $f(E \setminus \{e\}) = f(E)$, then

$$S_G(u,v) = S_{G\setminus e}(u,v) + S_{G\setminus e}(u,v)$$

Every connected graph other than those we put in our basis has an edge e that falls into one of these three cases. So we can prove (4) by induction on them. The details convey why we need to use the particular value $\alpha = -\sqrt{2}i$ but are otherwise straightforward and tedious, so we've put them in a longer PDF version. Since the equation (3) for S_G involves no recursion, this also proves that the recursive definition of $Q_G(x)$ is confluent.

Note how the sum in the case (c) echoes the sum defining the Tutte polynomial, but with "explosion" in place of ordinary graph contraction. A more salient difference is that whereas the Tutte polynomial is the same on all *n*-vertex trees, $Q_G(x)$ differs on them.

What Does It All Mean?

As remarked in Noble's paper, Oxley and Whittle noted the significance of a host of specializations of the $S_G(u, v)$ polynomial. We suppose G has n nodes with ℓ isolated, so $f(E) = n - \ell$, and we put m = |E|. The first two presume $\ell = 0$.

- 1. $S_G(0,0)$ is the number of perfect matchings of G.
- 2. $S_G(0,1)$ is the number of spanning subsets of E (not necessarily spanning trees).
- 3. $S_G(1,0)$ is the number of (partial) matchings of G.
- 4. $S_G(-u, -v) = (-1)^{n-\ell} S_G(u, v).$
- 5. $S_G(\frac{1}{x}, x) = (1 + x^2)^m x^{\ell n}$ (for $x \neq 0$).
- 6. The generating function $\sum_{k\geq 0} m_k x^k$ for the number m_k of matchings of size k equals $x^{(n-\ell)/2} S_G(\frac{1}{\sqrt{x}}, 0)$ (valid for real $x \neq 0$).
- 7. The generating function $\sum_{k\geq 0} r_k x^k$ for the number r_k of subsets of E spanning k vertices equals $x^{n-\ell}S_G(\frac{1}{x}, 1)$ (again valid for real $x \neq 0$).

Also interesting is that if $\ell = 0$ and we delete each of the *m* edges independently with probability (1 - p), then the probability that the deletions did not cause any isolated vertices is

$$(1-p)^{m-n/2}p^{n/2}S_G(0,\sqrt{\frac{p}{1-p}}).$$

Of course, this is classical probability. What interests us here is the import of S_G for quantum amplitude and probability. We have already observed in previous posts that $Q_G(1)$ gives the amplitude for an outcome in a special kind of quantum circuit. This means that $S_G(\alpha, -\alpha)$ gives the same information, where $\alpha^2 = -2$.

We are curious about is the significance of $S_G(\alpha x, -\alpha)$ for other values of x besides x = 1. The complex value $\alpha = -\sqrt{2}i$ takes us outside the real-valued domain of Noble's paper. His proof that most real cases are #P-hard to compute does not extend because $\alpha^2 = -2$, which causes a denominator in his proof to vanish. Thus $S_G(\alpha x, -\alpha)$ and hence $Q_G(x)$ may be polynomial-time computable for various other real x.

The specialization $Q_G(x) = S_G(\alpha x, -\alpha)$ (times other easily-computed factors) does not seem to intersect with any of the above cases. Hence the field is wide open for finding new interpretations of it. Whatever we find, however, is bound to relate to the analysis of quantum circuits. It might help fulfill the aim in our post drawing analogy to Gustav Kirchhoff's laws for electrical circuits.

Open Problems

How useful is the matroid-based framework for analyzing graph entities associated to quantum circuits?

We had thought to extend it by analogy with the Tutte polynomial T(x, y) having base monomials $x^q y^r$ for graphs composed of q "bridge" edges and r loop edges at otherwise-isolated nodes. One can base a polynomial $R_G(x, y, z, w)$ on monomials

$$x^{\ell}y^{r}z^{s}w^{t}$$

for G composed of ℓ isolated nodes, r disjoint single-node loops, s circles, and t "wisps." The recursion is the same:

$$R_G(x, y, z, w) = R_{G \setminus e}(x, y, z, w) - \frac{1}{f(e)} R_{G \setminus e}(x, y, z, w).$$

The point is that in the explosion case, the inclusion of the factor w^2 if the explosion leaves two wisps, wz if it leaves a wisp and a circle, or z^2 for two circles, keeps R_G homogeneous of degree n for an n-vertex graph. The conditions for this recursion to be confluent, however, essentially leave something equivalent to $Q_G(x)$ with w as a homogenizing variable. In particular, this idea appears not to yield a two-variable polynomial that gives more leverage.

Extra: Rest of the Main Proof

Proof. The game is to instantiate the three recursion cases of $S_G(u, v)$:

 $\begin{array}{lll} S_{G}(u,v) &=& S_{G\backslash e}(u,v) + vS_{G\backslash\backslash e}(u,v) & (\text{when } e \text{ is a loop}) \\ S_{G}(u,v) &=& uS_{G\backslash e}(u,v) + S_{G\backslash\backslash e}(u,v) & (\text{when } e \text{ is a pendant edge}) \\ S_{G}(u,v) &=& S_{G\backslash e}(u,v) + S_{G\backslash\backslash e}(u,v) & (\text{when } e \text{ is a normal edge}) \end{array}$

with $u = \alpha x$ and $v = -\alpha$, where $\alpha = -\sqrt{2}i$. According to these three respective cases (a,b,c) we analyze as follows.

(a) No isolated node is introduced either by removing or exploding e, so the $(\alpha x)^{\ell}$ term factors through and we can ignore it. Forming $G \setminus e$ reduces n by 1. Thus we get:

$$Q_{G}(x) = Q_{G \setminus e}(x) - Q_{G \setminus e}(x)$$

= $(\frac{1}{\alpha})^{n} S_{G \setminus e}(\alpha x, -\alpha) - (\frac{1}{\alpha})^{n-1} \alpha S_{G \setminus e}(\alpha x, -\alpha)$
= $(\frac{1}{\alpha})^{n} [S_{G \setminus e}(\alpha x, -\alpha) + (-\alpha) S_{G \setminus e}(\alpha x, -\alpha)]$
= $(\frac{1}{\alpha})^{n} S_{G}(\alpha x, -\alpha).$

(b) Removing *e* causes one more isolated node, but while exploding *e* reduces *n* by 2, it does not isolate any nodes, so:

$$Q_{G}(x) = Q_{G\backslash e}(x) - \frac{1}{2}Q_{G\backslash\backslash e}(x)$$

$$= (\frac{1}{\alpha})^{n}S_{G\backslash e}(\alpha x, -\alpha)\alpha x - \frac{1}{2}(\frac{1}{\alpha})^{n-2}\alpha S_{G\backslash\backslash e}(\alpha x, -\alpha)$$

$$= (\frac{1}{\alpha})^{n}[S_{G\backslash e}(\alpha x, -\alpha)\alpha x - \frac{1}{2}\alpha^{2}S_{G\backslash\backslash e}(\alpha x, -\alpha)]$$

$$= (\frac{1}{\alpha})^{n}[(\alpha x)S_{G}(\alpha x, -\alpha) + S_{G\backslash\backslash e}(\alpha x, -\alpha)]$$

$$= (\frac{1}{\alpha})^{n}S_{G}(\alpha x, -\alpha).$$

(c) Here removing e causes no more isolated nodes. Nor does exploding e, though we should note that exploding one edge of the three-node triangle graph creates a double-loop at the opposite vertex w. This is equivalent to isolating w, but the equivalence is already handled by our treatment of the base cases and by multiplicativity for disjoint components. So we can calculate:

$$Q_{G}(x) = Q_{G\backslash e}(x) - \frac{1}{2}Q_{G\backslash\backslash e}(x)$$

$$= (\frac{1}{\alpha})^{n}S_{G\backslash e}(\alpha x, -\alpha) - \frac{1}{2}(\frac{1}{\alpha})^{n-2}\alpha S_{G\backslash\backslash e}(\alpha x, -\alpha)$$

$$= (\frac{1}{\alpha})^{n}[S_{G\backslash e}(\alpha x, -\alpha)\alpha x - \frac{1}{2}\alpha^{2}S_{G\backslash\backslash e}(\alpha x, -\alpha)]$$

$$= (\frac{1}{\alpha})^{n}[(\alpha x)S_{G}(\alpha x, -\alpha) + S_{G\backslash\backslash e}(\alpha x, -\alpha)]$$

$$= (\frac{1}{\alpha})^{n}S_{G}(\alpha x, -\alpha).$$

This completes the proof.

Extra: Direct Proof of a(G) as a Generalized Tutte Invariant

We show how to represent the amplitude a(G) of a graph (or mgraph) G as a generalized Tutte invariant. We could infer this from $S_G(u, v)$ via our characterization of $Q_G(x)$ but we show it directly for a(G). We want to capture the numerator $c_0 - c_1$, where c_0 is the count of colorings that make an even number of B-B edges and c_1 gives the count of colorings that make an odd number of B-B edges.

With the rank function f_G defined as above, We show that a(G) falls into the first category of Theorem 4.1 in Noble's paper (which is Proposition 3.8 in Oxley and Whittle's with parameters

$$(r, s, t; a, b, c, d; m, n) = (1/2, -1, 0; 1, -1, 1, -1/2; 1, -1/2)$$

This gives

$$a(G) = \left(-\frac{1}{2}\right)^{n/2} S(f_G; -\sqrt{2}i, \sqrt{2}i),$$

where

$$S(f_G; x, y) = \sum_{A \subseteq E} x^{f(E) - f(A)} y^{2|A| - f(A)}$$

This in turn further simplifies to

$$a(G) = \sum_{A \subseteq E} \frac{(-2)^{|A|}}{2^{f_G(A)}}$$

Noble shows that computing $S(f_G; x, y)$ is #P-hard for any constant rational x, y whenever $xy \neq 1$. However, our complex irrational point $(-\sqrt{2}i, \sqrt{2}i)$ has xy = 2 and evades his proof because having $y^2 = -2$ makes a denominator vanish.

Following Noble's paper, let \mathcal{M} denotes the class of all graphic 2-polymatroids and call an edge e an *m*-separator if the endpoints of e and the set of endpoints of edges in $E \setminus e$ are disjoint—i.e., if e is an isolated edge.

Then $\phi : \mathcal{M} \to \mathbb{C}$ is said to be a generalized Tutte invariant (for graphic 2-polymatroids) if there exist constants $(r, s, t, a, b, c, d, m, n) \in \mathbb{C}^9$ such that

$$\phi(U_{2,1}) = r, \phi(U_{0,1}) = s, \phi(U_{1,1}) = t,$$

and for any graphic 2-polymatroid (E, f),

$$\phi(f) = \phi(f \setminus (E \setminus e))\phi(f \setminus e)$$
 if e is a separator of f;

and if e is not an m-separator,

$$\phi(f) = \begin{cases} a\phi(f \setminus e) + b\phi(f/e), & \text{if } f(E \setminus e) = f(E) \text{ and } f(e) = 1; \\ c\phi(f \setminus e) + d\phi(f/e), & \text{if } f(E \setminus e) = f(E) - 1 \text{ and } f(e) = 2; \\ m\phi(f \setminus e) + n\phi(f/e), & \text{if } f(E \setminus e) = f(E) \text{ and } f(e) = 2. \end{cases}$$

Note how this definition tracks the recursion cases for S_G in the above full proof. We imitate the two-term recursion on edge deletion and edge explosion for $c(G) = c_0 - c_1$ (so that $a(G) = c(G)/2^{|V|}$):

$$\begin{split} c(G) &= c(G) + c(G) \\ u, v \text{ are both black} & \text{at least one of } u, v \text{ is white} \\ &= c(G) + c(G \setminus e) \\ u, v \text{ are both black} & \text{at least one of } u, v \text{ is white} \\ &= c(G \setminus e) - c(G \setminus e) \\ \text{at least one of } u, v \text{ is white} & u, v \text{ are both black} \\ &= c(G \setminus e) - 2c(G \setminus e) \\ u, v \text{ are both black} \\ &= c(G \setminus e) - 2c(G \setminus e), \end{split}$$

and in turn

$$a(G) = \frac{c(G \setminus e)}{2^{|V|}} - \frac{2}{4} \cdot \frac{c(G/e)}{2^{|V|-2}} = a(G \setminus e) - \frac{1}{2}a(G \setminus e).$$

If e is a self-loop, we can use a similar argument to derive

$$a(G) = a(G \setminus e) - a(G \setminus e).$$

Now we can start working out those constants for $\phi(G) = a(G)$. Recall that the rank value f(A) in a graph G is the number of distinct endpoints of edges in set A.

$$r = a(e) = \frac{1}{2}$$

$$s = a(\bigcirc) = -1$$

$$t = a(loop) = 0.$$

If e is not a separator, we only have two cases to consider–if e is a self-loop or an edge connecting two vertices:

- if $f(E \setminus e) = f(E)$ and f(e) = 1, then this edge e is a self-loop and from above we have a = 1, b = -1;
- if $f(E \setminus e) = f(E) 1$ and f(e) = 2, or $f(E \setminus e) = f(E)$ and f(e) = 2, then e is an ordinary edge making c = m = 1 and $d = n = -\frac{1}{2}$.

Overall, this gives the set of parameters and hence the desired Tutte representation for a(G) as stated above.