Symmetric Circuits for Rank Logic

Anuj Dawar and Gregory Wilsenach

University of Cambridge Computer Laboratory
{anuj.dawar, gregory.wilsenach} @cl.cam.ac.uk

April 13, 2017

Abstract

Anderson and Dawar (2014) showed that fixed-point logic with counting (FPC) can be characterised by uniform families of polynomial-size symmetric circuits. We give a similar characterisation for fixed-point logic with rank (FPR) by means of symmetric circuits including rank gates. This analysis requires a significant extension of previous methods to deal with gates computing Boolean functions which are not themselves symmetric. In particular, we show that the support theorem of Anderson and Dawar can be extended to circuits whose gates satisfy a property that we term "matrix-symmetry".

1 Introduction

Circuit complexity has been used as an alternative approach for studying algorithmic complexity. This method has proved useful in descriptive complexity as well, with some authors, e.g. Otto [11] and Denenberg et al. [6], developing circuit-based characterisations for logics. In both these cases symmetric circuits are studied, that is circuits that take in finite structures over some universe and where permutations of the universe of the input structure are reflected as automorphisms of the circuit. These symmetric circuits provide a natural circuit interpretation of many of the symmetries found in the logic context.

Anderson and Dawar [1] studied the expressive power of P-uniform families of symmetric circuits, where a P-uniform family of circuits is a family $(C_n)_{n\in\mathbb{N}}$ such that the function $n \mapsto C_n$ is polynomial-time computable. They found that such families defined over a complete Boolean basis with a majority function completely characterised fixed-point logic with counting (FPC).

While we know that FPC does not capture PTIME [4], FPC does capture PTIME over many classes of structures [9] and many natural PTIME problems are expressible FPC (e.g. Maximum Matching [2]). While FPC is thus an important logic of interest for its own sake, FPC also plays a role as a logic from which other important logics of study are defined. The particular logic of interest in this paper is *fixed-point logic with rank* (FPR), introduced by Dawar et al. [5] and defined as an extension of FPC that includes operators that can define the rank of a definable matrix over a fixed finite field. This extension was prompted by the work of Atserias et al. [3], who had shown that that some of the most difficult to express problems in PTIME (and not expressible in FPC) were reducible to the general problem of solving systems of linear equations over prime fields. Indeed, problems of this sort have remained the primary source of difficult-to-express problems in descriptive complexity, motivating the modern study of FPR.

It is worth noting the logic defined by Dawar et al. introduces for each prime a separate operator that computes the rank of the matrix over that prime. It was shown by Grädel and Pakusa [7] that this logic does not capture PTIME. Instead, they present a strictly more expressive alternative rank logic which includes only a single rank operator that takes in both the matrix and a specific prime over which to compute the rank as input. In this paper when we refer to FPR we are referring to this more expressive version of Graädel and Pakusa.

In this abstract we review the work of Anderson and Dawar on symmetric circuits, and extend their analysis by broadening the basis of functions they consider to include so-called 'matrix-symmetric' functions. This class of functions includes important non-symmetric functions, e.g. the rank of a matrix, and this allows us to study symmetric circuits with gates that compute rank. Our main result is a circuit characterisation for FPR. In particular, we show that P-uniform families of symmetric circuits with rank gates characterise FPR. This requires a significant advance on the methods of [1].

2 Background

A circuit for structures, as given by Anderson and Dawar, is defined for a fixed relational vocabulary τ, a Boolean basis of symmetric functions $\mathbb{B}$ and some fixed universe of size n. The input gates are taken to be the formal graph of the relational symbols over the universe $[n]$, i.e. gates labelled by $R(\vec{x})$ where $\vec{x} \in [n]^{\text{arty}(R)}$. The input to the circuit is a finite τ-structure $\mathcal{A}$ of cardinality n.

Evaluation of the circuit proceeds by first choosing a bijection δ from the universe of $\mathcal{A}$ to $[n]$ and then, for each input gate, using the interpretation of the relevant relational symbol in $\mathcal{A}$ and the bijection δ to evaluate the gate. Recursing through the circuit and evaluating the internal gates using the given semantics for the symbols in the Boolean basis allows each gate in the circuit to be evaluated.

We say that such a circuit is *invariant* if its output does not depend on the choice of δ.

A *symmetric* circuit is a circuit such that every permutation on the universe $[n]$, each of which induces a permutation on the input gates, extends to an automorphism of the circuit. A symmetric circuit is necessarily invariant.

It is important to note that the word 'symmetric' is used in two different ways here. When applied to a circuit the above definition is used, but when applied to a Boolean function it denotes a function whose output depends only on the number of 1's in its input. The meaning is always clear from context.

The main result of [1] is the following characterisation theorem.

Theorem 1. *For any relational vocabulary τ, a property of finite τ-structures is decided by a P-uniform family of symmetric circuits with majority gates if, and only if, it is expressible in FPC.*

The difficult direction in the proof is in taking families of circuits and defining an equivalent sentence of FPC. It relies crucially on the notion of a *support*.

Definition 2. *A set $S \subseteq [n]$ is called a support for a gate g if every permutation that fixes S point-wise has an extension that fixes g.*

It is shown that for polynomially-bounded circuit families each gate has a constant size support. In fact, a stronger result is established, requiring only that the orbit for each gate under the action induced by permutations of the universe of the input structure be polynomially bounded.

Theorem 3. *For large enough n and constant k, if C is a symmetric circuit with gates such that for each gate g in C the orbit is bounded by n^k then each gate has a a support of size $O(k)$.*

One can then show that when evaluating the circuit for an input structure and a particular choice of bijection δ, the evaluation of the gate g depends only those elements of the universe δ assigns to the support of g. This allows each gate g to be associated with a relation consisting of all those assignments to the support of g that make g evaluate to true. These relations can then be defined through structural induction on the circuit, which can be done in FPC using the fixed-point operator. The induction crucially uses the fact that the Boolean function computed by each gate is symmetric.

Finally, the Immerman-Vardi theorem [10] and the uniformity condition on the family of circuits, along with the above observations, allows one to show that for a finite τ-structure the appropriate circuit from the given family can be defined and evaluated in FPC, completing the direction and proving the result.

3 Main Results: Circuits with Matrix-Symmetric Gates

Many Boolean functions of interest, particularly the rank of a matrix, are not symmetric functions. As such, we extend the analysis of symmetric circuits to circuit families defined over Boolean bases that draw from a broader class of functions. In particular we consider the addition of Boolean functions that are 'matrix-symmetric', in the sense that they are invariant under row/column permutations of their input. We show that P-uniform families of symmetric circuits with rank gates entirely characterise FPR.

We first show that no expansion of a basis consisting of only symmetric functions can increase the computational power of the symmetric circuit model. This shows that we need to consider non-symmetric functions in order to develop the desired characterisation.

Theorem 4. *Suppose (C_n) is a family of symmetric circuits over some set of symmetric functions. Then there is an equivalent family of symmetric circuits with only a polynomial blowup in size over the standard basis with majority that computes the same function.*

We formally define a matrix-symmetric function.

Definition 5. *A function $f : \{0,1\}^{A\times B} \to \{0,1\}$ is matrix-symmetric if for all $\delta : A \times B \to \{0,1\}$ and for all $\alpha, \beta \in \boldsymbol{Sym}_A \times \boldsymbol{Sym}_B$ have that $f(\delta) = f((\alpha,\beta)\cdot\delta)$.*

We consider a P-uniform family of symmetric circuits with rank gates (i.e. gates labelled by functions of the form $f : \{0,1\}^{A\times B} \to \{0,1\}$ that evaluates to 1 if, and only if, the rank of the input matrix for a certain prime is above a fixed value). It is easy to show that for any sentence in FPR an equivalent family of such circuits exists. It remains to prove the reverse direction.

In proving this direction we prove an analogue of the support theorem for circuits with matrix-symmetric functions. As noted above, in the original proof of the result, the key inductive step crucially relies on the fact that the basis consists only of symmetric functions. Our extension consists in showing that when the inputs to a matrix-symmetric gate g have small support, and the orbit of g is small, then g must also have small support. This requires a careful analysis of how supports interact with direct products of symmetric groups (of the form $\mathbf{Sym}_A \times \mathbf{Sym}_B$) rather than just the symmetric group.

Theorem 6. *For large enough n and constant k, if C is a symmetric circuit with matrix-symmetric gates such that for each gate g in C the orbit is bounded by n^k then each gate has a a support of size $O(k)$.*

We similarly show that for any circuit C_n, input structure $\mathcal{A}$ of size n, and bijection δ from the structure's universe to $[n]$, the evaluation of matrix-symmetric gates is determined entirely by which elements in the universe are assigned by δ to the support. Again, we can associate with each gate a relation consisting of those assignments that cause the gate to evaluate to true, and seek to prove that these relations can be defined inductively in FPR. We now restrict ourselves to the case where the only matrix-symmetric gates in the circuit are rank gates. The inductive definition of these relations in the proof of the previous result explicitly relies on the symmetry of the basis functions. In the matrix-symmetric (or rank) case, we rely instead on the study of 'row supports' and 'column supports'. For a gate h, a child of g, a *row support* is a set $r \subseteq [n]$ such that any permutation that fixes r point-wise also fixes the row of h in the matrix labelling at g. We define a *column support* similarly. For a fixed assignment to the support of g, we use assignments to these row and column supports as indices in order to define a matrix in FPR. We show that this matrix has the same rank as any matrix formed by evaluating the child gates of g and computing the rank of the resultant 0-1 matrix. The following technical lemma, which is the key inductive step in our argument, summarises this result.

Lemma 7. *Let C_n be a circuit, g be a rank gate and $\mathcal{A}$ be an appropriate input structure with universe U. Let α be an injection from the support of g to U. Let $\delta : U \to [n]$ be a bijection that assigns elements of the universe of $\mathcal{A}$ to the universe of the circuit. Then there exists a matrix M_α definable in FPR such that for any δ where δ^{-1} agrees with α on the support of g it follows that L^δ, the 0-1 matrix formed by evaluating each of the children of g using using δ, has the same rank as M_α.*

This lemma allows us to inductively define the required relations, which in turn allows for a given circuit to be evaluated in FPR. We similarly make use of the Immerman-Vardi theorem in order to generate the required circuit in FPR, and so prove our main result.

Theorem 8. *For any relational vocabulary τ, a property of finite τ-structures is decided by a P-uniform family of symmetric circuits with rank gates if, and only if, it is expressible in FPR.*

4 Concluding Remarks and Future Work

In this paper we extend the study of symmetric circuits through the introduction of matrix-symmetric functions that allow us to define a symmetric circuit model that characterises FPR. This approach raises

a number of questions about the power of related models. For example, what kinds of queries can families of symmetric circuits with arbitrary matrix-symmetric functions define? Moreover, what about extension of symmetric circuits that include tensor-symmetric functions, or functions that are symmetric with respect to particular subgroups of the symmetric group? These are a few natural extensions that merit investigation.

It is also worth considering if a similar circuit model could be used to characterise Choiceless Polynomial Time (CPT). The Polynomial-time Interpretation Logic (PIL) of Grädel [8] suggests one approach, but the obvious circuit implementation seems to break symmetry. Alternatively, perhaps weaker notions of symmetry, ones that better reflect those in the definition of CPT, might be an avenue for producing useful circuit models.

References

[1] M. Anderson and A. Dawar. On symmetric circuits and fixed-point logics. *Theory of Computing Systems*, 60(3):521–551, 2017.

[2] M. Anderson, A. Dawar, and B. Holm. Maximum matching and linear programming in fixed-point logic with counting. In *2013 28th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 173–182, 2013.

[3] A. Atserias, A. Bulatov, and A. Dawar. Affine systems of equations and counting infinitary logic. *Theoretical Computer Science*, 410(18):1666–1683, 2009.

[4] J. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.

[5] A. Dawar, M. Grohe, B. Holm, and B. Laubner. Logics with rank operators. In *2009 24th Annual IEEE Symposium on Logic In Computer Science (LICS)*, pages 113–122, 2009.

[6] L. Denenberg, Y. Gurevich, and S. Shelah. Definability by constant-depth polynomial-size circuits. *Information and Control*, 70(2):216–240, 1986.

[7] E. Grädel and W. Pakusa. Rank logic is dead, long live rank logic! In *2015 24th Annual Conference on Computer Science Logic, (CSL)*, pages 390–404, 2015.

[8] E. Grädel, W. Pakusa, S. Schalthöfer, and L. Kaiser. Characterising choiceless polynomial time with first-order interpretations. In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 677–688, 2015.

[9] M. Grohe. Fixed-point definability and polynomial time on graphs with excluded minors. In *2010 25th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 179–188, July 2010.

[10] N. Immerman. Relational queries computable in polynomial time. *Information and Control*, 68(1-3):86 – 104, 1986.

[11] M. Otto. The logic of explicitly presentation-invariant circuits. In *1996 10th International Workshop, Annual Conference on Computer Science Logic (CSL)*, pages 369–384. Springer, Berlin, Heidelberg, 1997.