JOHANNES KEPLER
UNIVERSITY LINZ

MAXIMALITY OF REVERSIBLE GATE SETS

Various closures

Tim Boykett
10 July 2020
Algebra

JOHANNES KEPLER UNIVERSITY LINZ

PREREQUISITES

Background

Let A be a finite set. $Sym(A) = S_A$ is the set of permutations or bijections of A, $Alt(A)$ the set of permutations of even parity. Let $B_n(A) = Sym(A^n)$ and $B(A) = \bigcup_{n \in \mathbb{N}} B_n(A)$. We call $B_n(A)$ the set of n-ary reversible gates on A, $B(A)$ the set of reversible gates.

For $\alpha \in S_n$, let $\pi_\alpha \in B_n(A)$ be defined by $\pi_\alpha(x_1, \ldots, x_n) = (x_{\alpha^{-1}(1)}, \ldots, x_{\alpha^{-1}(n)})$. We call this a wire permutation.

Let $\Pi = \{\pi_\alpha | \alpha \in S_n,\ n \in \mathbb{N}\}$. In the case that α is the identity, we write $i_n = \pi_\alpha$, the n-ary identity.

Let $f \in B_n(A)$, $g \in B_m(A)$. Define the parallel composition as $f \oplus g \in B_{n+m}(A)$ with

$$(f \oplus g)(x_1, \ldots, x_{n+m}) = \\ (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n), \\ g_1(x_{n+1}, \ldots, x_{n+m}), \ldots, g_m(x_{n+1}, \ldots, x_{n+m}))$$

For $f, g \in B_n(A)$ we can compose $f \bullet g$ in $Sym(A^n)$. If they have distinct arities we “pad” them with identity, for instance $f \in B_n(A)$ and $g \in B_m(A)$, $n < m$, then define $f \bullet g = (f \oplus i_{m-n}) \bullet g$ and we can thus serially compose all elements of $B(A)$.

Definition

We call a subset $C \subseteq B(A)$ that includes Π and is closed under $\oplus$ and $\bullet$ a reversible Toffoli algebra (RTA).

Let C be an RTA. We write $C^{[n]} = C \cap B_n(A)$ for the elements of C of arity n.

Example

Let q be a prime power, $GF(q)$ the field of order q, $AGL_n(q)$ the collection of affine invertible maps of $GF(q)^n$ to itself. We note that for all $m \in \mathbb{N}$, $AGL_n(q^m) \leq AGL_{nm}(q)$. For a prime p, let $\mathrm{Aff}(p^m) = \bigcup_{n\in\mathbb{N}} AGL_{nm}(p)$ be the RTA of affine maps over $A = GF(p)^m$.

Definition

We say that an RTA $C \leq B(A)$ is borrow closed if for all $f \in B(A)$, $f \oplus i_1 \in C$ implies that $f \in C$.

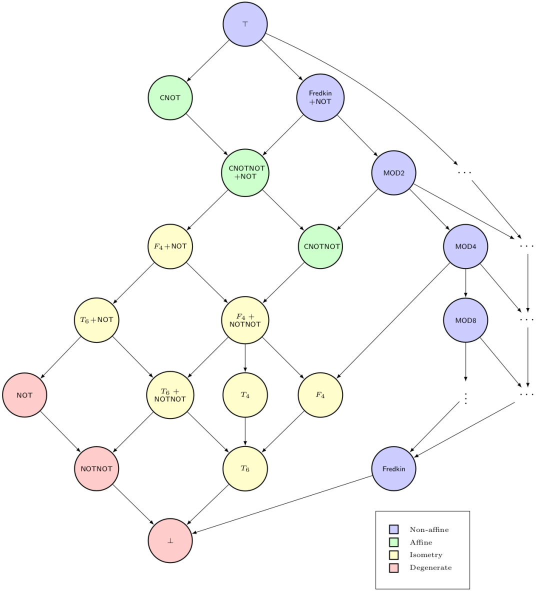
Definition

We say that an RTA $C \leq B(A)$ is ancilla closed if for all $f \in B_n(A)$, $g \in C^{[n+1]}$ with some $a \in A$ such that for all $x_1, \ldots, x_n \in A$, for all $i \in \{1, \ldots, n\}$, $f_i(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_n, a)$ and $g_{n+1}(x_1, \ldots, x_n, a) = a$ implies that $f \in C$.

If an RTA is ancilla closed then it is borrow closed.

For any prime power q, $\mathrm{Aff}(q)$ is borrow and ancilla closed.

$|A| = 2$ ancilla closure (AGS 2015)



Theorem (Liebeck, Praeger, Saxl 1987)

Let $n \in \mathbb{N}$. Then the maximal subgroups of S_n are conjugate to one of the following G.

1. *(alternating)* $G = A_n$
2. *(intransitive)* $G = S_k \times S_m$ *where* $k + m = n$ *and* $k \neq m$
3. *(imprimitive)* $G = S_m wr S_k$ *where* $n = mk$, $m, k > 1$
4. *(affine)* $G = AGL_k(p)$ *where* $n = p^k$, p *a prime*
5. *(diagonal)* $G = T^k.(Out(T) \times S_k)$ *where* T *is a nonabelian simple group,* $k > 1$ *and* $n = |T|^{(k-1)}$
6. *(wreath)* $G = S_m wr S_k$ *with* $n = m^k$, $m \geq 5$, $k > 1$
7. *(almost simple)* $T \triangleleft G \leq Aut(T)$, $T \neq A_n$ *a nonabelian simple group,* G *acting primitively on* A

Moreover, all subgroups of these types are maximal when they do not lie in A_n*, except for a list of known exceptions.*

Clones

Let A be a finite set. $\mathcal{O}(A)$ is the full clone of all mappings $f : A^n \to A$ for all $n \in \mathbb{N}$.

A clone of A is a set of mappings $f : A^n \to A$ closed under some natural operations.

Theorem (Rosenberg)

Let A be a finite set. Then the maximal subclones of $\mathcal{O}(A)$ are one of the following.

1. *monotone mappings, that is respecting a bounded partial order on A*
2. *respecting a graph of prime length loops*
3. *respecting a nontrivial equivalence relation*
4. *affine mappings for a prime p: that is, respecting the relation $\{(a, b, c, d) \mid a + b = c + d\}$ where $(A, +)$ is an elementary abelian group*
5. *respecting a central relation*
6. *respecting a h-generated relation*

If $R \subseteq A^k$ is a k-ary relation, we write $Pol(R)$ as the polymorphisms respecting R.

Example: $A = \{1, 2, 3\}$ with $1 \leq 2 \leq 3$. Then $Pol(\leq)$ are the monotone functions on A.

RTA Duality

Let $(M, +)$ be a commutative monoid. Let $w : A^k \to M$ be a mapping called a weight function. Let $f \in B_n(A)$. We say f respects w, $f \triangleright w$, if for every $a \in A^{k \times n}$, $\sum_i w(a_{1i}, \ldots, a_{ki}) = \sum_i w(f_i(a_{11}, \ldots, a_{1n}), \ldots, f_i(a_{k1}, \ldots, a_{kn}))$.

Then $Pol(w) = \{f \in B(A) \mid f \triangleright w\}$ are the mappings that conserve w.

Theorem (Jerabek)

Let A be a finite set. Then the sub RTAs of $B(A)$ are defined by a suitably closed collection of weight functions.

Example: $(\mathbb{B}, \wedge)$ is a monoid, let $R \subset A^k$ be a relation $w_R(a_1, \ldots, a_k)$ is true iff $(a_1, \ldots, a_k) \in R$. Then $Pol(w_R)$ are those mappings where each index is in $Pol(R)$.

Example: $(\mathbb{N}_0, +)$ is a monoid, select $a \in A$, then $w : A \to \mathbb{N}$ with $w(x) = 1$ if $x = a$ and zero otherwise. Then $Pol(w)$ is the collection of a-conservative mappings.

MAXIMAL RTA

Unique index

Lemma

Let A be a finite set. Let M be a maximal sub RTA of $B(A)$. Then $M^{[i]} \neq B_i(A)$ for exactly one i and $M^{[i]}$ is a maximal subgroup of $B_i(A) = Sym(A^i)$.

Maximality

Theorem

Let A be a finite set. Let M be a maximal sub RTA of $B(A)$. Then $M^{[i]} \neq B_i(A)$ for exactly one i and $M^{[i]}$ belongs to one of the following classes:

1. $i = 1$ *and* $M^{[1]}$ *is one of the classes in Theorem 2.*
2. $i = 2$, $|A| = 3$, *and* $M^{[2]} = AGL_2(3)$ *(up to conjugacy)*
3. $i = 2$, $|A| \geq 5$ *is odd and* $M^{[2]} = S_A wr S_2$
4. $i = 2$, $|A| \equiv 2 \mod 4$ *and* $M^{[2]} = S_A wr S_2$
5. $i = 2$, $|A| \equiv 0 \mod 4$ *and* $M^{[2]} = Alt(A^2)$
6. $i \geq 3$, $|A|$ *is even and* $M^{[i]} = Alt(A^i)$

BORROW AND ANCILLA CLOSURE

Lemma

Let $M \leq B(A)$ *be a maximal borrow or ancilla closed RTA. Then there exists some* $k \in \mathbb{N}$ *such that for all* $i < k$*,* $M^{[i]} = B_i(A)$ *and for all* $i \geq k$*,* $M^{[i]} \neq B_i(A)$*.*

Lemma

Let $|A|$ be odd. Then M maximal with index $k = 1, 2$ are the only options.

Lemma

Let $|A| = 2$. Then M maximal with index $k = 1, 2, 3$ are the only options and for $i > k$, $M^{[i]} \neq Alt(A^i)$.

Lemma

Let $|A| \geq 4$ be even. Then M maximal with index $k = 1, 2$ are the only options and for $i > k$, $M^{[i]} \neq Alt(A^i)$.

Lemma

For $|A| \geq 5$, the degenerate RTA $Deg(A)$ generated by $B_1(A)$ is a maximal borrow closed RTA and maximal ancilla closed RTA of index 2.

Lemma

Let A be of prime power order. Then $\mathrm{Aff}(A)$ is a maximal borrow closed RTA and a maximal ancilla closed RTA of index 3 for $|A| = 2$, index 2 for $|A| = 3, 4$ otherwise index 1.

Definition

Let $D \subset A$. Define $Stab_D(A) = \{f \in B_n(A) \mid f(D^n) = D^n\}$ the set-wise stabilizer of D.

Lemma

Let $D \subset A$ nontrivial. Then $Stab_D(A)$ is a maximal borrow closed RTA of index 1.

Definition

Let $a \in A$, $n \in N$, define $w_a : A \to \mathbb{Z}_n$ by $w_a(x) = 1$ if $x = a$ otherwise $w_a(x) = 0$. Define $Cons_{a,n}(A) = Pol(w_a)$, the mod-n a-conserving mappings.

Conjecture

Let p be prime, then $Cons_{a,p}(A)$ is an index 1 maximal borrow closed and a maximal ancilla closed RTA, except when $|A| = 2$ and $p = 2$.

END

JOHANNES KEPLER
UNIVERSITY LINZ