AAQDD – Abstract additive quantum decision diagrams

M. Leroy, R. Vilmart

February 17, 2025

Contents

Chapter 1

Complex intervals arithmetics

1.1 Generalities

The purpose of quantum decision diagrams is to provide a more efficient way to store and manipulate quantum states of a finite number of qubits. A n-qubit state is indeed traditionally represented as an element of $\mathbb{C}^{2^n}$ (with norm 1), which takes exponential space as n grows. Abstract states will be in this part defined similarly, but with complex intervals instead of complex numbers.

1.1.1 Real intervals

The standard definition of real intervals is:

$$\forall a, b \in \mathbb{R}, [a, b] = \{x \in \mathbb{R} / \min(a, b) \leq x \leq \max(a, b)\}$$

From now on, the set of real intervals will be noted $\mathcal{A}_0(\mathbb{R})$. Of course, $\mathcal{A}_0(\mathbb{R}) \subset \mathcal{P}(\mathbb{R}) \subset \mathcal{P}(\mathbb{C})$. While not being sufficient to handle completely our operations on quantum states, caracterized by complex amplitudes, these real intervals will still be useful. Moreover, they are well-known and many papers already studied them.

1.1.2 Closure & operations

Let $E \subset \mathcal{P}(\mathbb{C})$ a set containing sets of $\mathbb{C}$ (later on, our intervals).

Definition 1.1 (closure)
The closure $\mathscr{C}$ of a set $a \in \mathcal{P}(\mathbb{C})$ is defined by

$$\mathscr{C}(a) = \bigcap_{\gamma \supset a \ \text{and} \ \gamma \in \mathcal{A}_0(\mathbb{C})} \gamma$$

Additionally, for any operator $\odot : {\mathcal{A}_0}^2 \to \mathcal{P}(\mathbb{C})$, we define the operator $\mathscr{C}(\odot) : {\mathcal{A}_0}^2 \to \mathcal{A}_0$ such that

$$\forall a, b \in \mathcal{P}(\mathbb{C}), a \ \mathscr{C}(\odot) \ b = \mathscr{C}(a \odot b)$$

Proposition 1.1 (colsure)
The closure is well-defined.

- *If $\odot$ is commutative, so is $\cdot$*

•

Definition 1.2 (operations)
Let $E \subset \mathcal{P}(\mathcal{C})$. We define for $\alpha, \beta \in \mathcal{P}(\mathbb{C})$ the following operations

$$\alpha \otimes \beta = \{ab; a \in \alpha, b \in \beta\}$$

$$\alpha \oplus \beta = \{a + b; a \in \alpha, b \in \beta\}$$

*Note that none of these sets are in E in the general case, despite it being the case for $E = \mathcal{A}_0(\mathbb{R})$. We define the **sum** in $\mathcal{A}_0$ to be $+ = \mathscr{C}(\oplus)$ and the **product** in $\mathcal{A}_0$ to be $\cdot = \mathscr{C}(\oplus)$. Additionally, we define the **join** $\sqcup = \mathscr{C}(\cup)$.*

Remarkably, in $+$ is the same as $\oplus$ and $\cdot$ is the same as $\otimes$. On complex intervals, we will see later that this is not necessarily the case.

Definition 1.3 (modulus)
For all α in E, we define when it exists $\forall \alpha \in E, |\alpha| = \sup\{|a|; a \in \alpha\}$.

This general case on a contextual set E leads to defining a **partial order** $\leq$, which really is the subset relation $\supset$, but implying that the sets are all intervals of the same interval set E. We easily get the following properties

i $\forall \alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathcal{A}_0, \alpha_1 \leq \alpha_2$ and $\beta_1 \leq \beta_2 \Rightarrow \alpha_1 + \alpha_2 \leq \beta_1 + \beta_2$

ii $\forall \alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathcal{A}_0, \alpha_1 \leq \alpha_2$ and $\beta_1 \leq \beta_2 \Rightarrow \alpha_1\alpha_2 \leq \beta_1\beta_2$

Note that in the case of $\mathcal{A}_0(\mathbb{R})$, the sum and product are **direct**, meaning that for all $\alpha, \beta \in \mathcal{A}_0^+, \alpha + \beta = \alpha \oplus \beta$ and $\alpha\beta = \alpha \otimes \beta$. To prove that the sum (respectively, the product) is direct, it is enough to prove that summing (respectively multiplying) two elements of E yields another element of E.

The operations $\oplus, \otimes, \sqcup, +$ and $\cdot$ are obviously commutative, but only $\oplus$ and $\otimes$ are always associative no matter the set E. Proving the directness of the sum or the product in E is hence a way to prove their associativity in E.

1.1.3 Remarkable subsets

Intervals of $\mathcal{A}_0(\mathbb{R})$, while being already unsifficient to fully cover the use of intervals in a quantum context, contain even more resricted subsets that will be useful in the next sections. The set of positive intervals $\mathcal{A}_0^+ = \mathcal{A}_0(\mathbb{R}) \cap \mathcal{P}(\mathbb{R})$ is remarkably convenient because it is working well with the operations defined above.

First, $\mathcal{A}_0^+$ is stable for $+$, $\cdot$ and $\sqcup$, meaning that using these operations on two elements of $\mathcal{A}_0^+$ results in another element of $\mathcal{A}_0^+$. Second, for all real number $0 \leq a_1 \leq b_1$ and $0 \leq a_2 \leq b_2$

$$[a_1, b_1] + [a_2, b_2] = [a_1 + a_2, b_1 + b_2]$$

$$[a_1, b_1][a_2, b_2] = [a_1a_2, b_1b_2]$$

Let $\mathcal{A}_0^{2\pi} = \mathcal{A}_0^+ \cap \mathcal{P}([0, 2\pi])$. While $\mathcal{A}_0^{2\pi}$ is not stable, it will be useful in section 1.3.

Theorem 1.1 (intervals of the exponential)
Let $\theta \in \mathcal{A}_0^+$, there is a unique $\varphi \in \mathcal{A}_0^{2\pi}$ such that

$$\exp(i\theta) = \exp(i\varphi)$$

Proof. There are unique $\theta^-, \theta^+, \mathbb{R}^+$ such that $\theta = [\theta^-, \theta^+]$ and $\theta^- \leq \theta^+$.

□

1.2 Cartesian intervals

1.2.1 Definition

Real intervals can be generalised to complex intervals naturally using the cartesian notation of complex numbers.

$$\forall x, y \in \mathbb{C}, [x, y] = \{a + ib; a \in [\mathrm{Re}(x), \mathrm{Re}(y)], b \in [\mathrm{Im}(x), \mathrm{Im}(y)]\}$$

Similarly to what can be done with real intervals, we can see complex numbers as complex intervals that only have one element, hence we might use $\mathbb{C}$ to be $\{[z, z]; z \in \mathbb{C}\}$. Now let $\mathcal{A}_0 = \{[x, y]; x, y \in \mathbb{C}\}$.

1.2.2 Operations

The basic operations on $\mathcal{A}_0$ (sum, product and join) are defined thanks to subsection **??**. Note that the product is not associative in $\mathcal{A}_0$, and that the sum is not distributive on the product:

Proposition 1.2 (growth)

$$\forall a, b \in$$

Proposition 1.3 (Sub-distributivity of the product)

$$\forall \alpha, \beta, \gamma \in \mathcal{A}_0, (\alpha + \beta)\gamma \subset \alpha\gamma + \beta\gamma$$

Proof.

$$\begin{aligned}
(\alpha + \beta)\gamma &= \{xc; x \in \{a + b; a \in \alpha, b \in \beta\}, c \in \gamma\} \quad \text{(by definition of the product)} \\
&= \{(a + b)c; a \in \alpha, b \in \beta, c \in \gamma\} \\
&= \{ac + bc; a \in \alpha, b \in \beta, c \in \gamma\} \\
&\subset \{ac + bd; a \in \alpha, b \in \beta, c, d \in \gamma\} \\
&\subset \{ac; a \in \alpha, c \in \gamma\} + \{bc; b \in \beta, c \in \gamma\} \quad \text{(by definition of the sum)} \\
&\subset \alpha\gamma + \beta\gamma
\end{aligned}$$

□

Proposition 1.4 (Sum)

$$\forall \alpha, \beta, \gamma, \delta \in \mathcal{A}_0 (\alpha \subset \gamma \text{ and } \beta \subset \delta) \Rightarrow \alpha + \beta \subset \gamma + \delta$$

and more generally

$$\forall n \in \mathbb{N}, \forall \alpha_1, ..., \alpha_n, \beta_1, ..., \beta_n \in \mathcal{A}_0, (\forall i \in \{1, ..., n\}, \alpha_i \subset \beta_i) \Rightarrow \sum_{i=1}^{n} \alpha_i \subset \sum_{i=1}^{n} \beta_i$$

Proof. □

1.2.3 Convex conservation

Proposition 1.5 (Convex conservation)
All complex intervals are convex.

Proof. Let $\alpha \in \mathcal{A}_0$ and $a, b \in \alpha$. Additionally let $t \in [0,1]$.

$$\begin{aligned}\mathrm{Re}(ta + (1-t)b) &= \mathrm{Re}(ta) + \mathrm{Re}((1-t)b) \\ &\leq t\mathrm{Re}(a) + (1-t)\mathrm{Re}(b) \quad (\text{since } t, 1-t \in \mathbb{R}) \\ &\leq \max(\mathrm{Re}(\alpha)) \quad \text{since } a, b \in \alpha\end{aligned}$$

The corresponding properties with a minimum or the imaginary part are proven very similarly, hence $ta + (1-t)b \in \alpha$. □

1.2.4 The minus operation

This gives *almost* us an ring structure for $(\mathcal{A}_0, +, \cdot)$, which we will use just next, and form now on we will note $0 = [0,0]$ and $1 = [1,1]$. However it is indeed not a ring because $(\mathcal{A}_0, +)$ is not a group. In fact, the exitence of an opposite (additive inverse) in $\mathcal{A}_0$ is replaced by the following property, which implies that almost no complex interval has an opposite:

$$\forall \alpha, \beta \in \mathcal{A}_0, \alpha \notin \mathbb{C} \Rightarrow \alpha + \beta \neq 0$$

Proof: Let $\alpha, \beta \in \mathcal{A}_0$, such that $\alpha \notin \mathbb{C}$. Let $b \in \beta$. Now, since $\alpha \notin \mathbb{C}$ there are at least two different complex numbers $x, y \in \mathbb{C}$ in α. Hence one of them $z \in \{x, y\}$ is different from $-b$, so $z + b \in \alpha + \beta$ and $z + b \neq 0$ and finally $\alpha + \beta \neq 0$. □

This implies the non-existence of an additive inverse for all non-constant intervals, which breaks any ring structure we could try to build on $+$. Despite that, we can still define a minus operation

$$\forall \beta \in \mathcal{A}_0, -\beta = \{-b; b \in \beta\}$$
$$\forall \alpha, \beta \in \mathcal{A}_0, \alpha - \beta = \alpha + (-\beta)$$

What is important keep in mind is that we cannot do things like "$\alpha + \beta = \gamma$ *so* $\alpha = \gamma - \beta$", for example if $\alpha = \beta = [0,1]$. Fundamentally, $\alpha - \alpha \neq 0$.

1.2.5 Partial order on intervals

We define the relation $\leq$ on $\mathcal{A}_0$ such that $\forall \alpha, \beta \in \mathcal{A}_0, \alpha \leq \beta \Rightarrow \alpha \subset \beta$. We easily get the following properties:

i $\forall \alpha, \beta \in \mathcal{A}_0, \alpha \leq \beta \Rightarrow \alpha^c \leq \beta^c$

ii $\forall \alpha, \beta, \gamma \in \mathcal{A}_0, \alpha\gamma \leq \beta\gamma$ and $\gamma \neq 0 \Rightarrow \alpha \leq \beta$

1.2.6 Centering

For all $\alpha \in \mathcal{A}_0$, we introduce $\mu(\alpha) \in \mathbb{C}$ the *middle* of α:

$$\mu(\alpha) = \frac{\min(\mathrm{Re}\ \alpha) + \max(\mathrm{Re}\ \alpha)}{2} + i\frac{\min(\mathrm{Im}\ \alpha) + \max(\mathrm{Im}\ \alpha)}{2}$$

This notion comes with the following properties:

i $\forall x \in \mathbb{C}, \mu([x,x]) = x$

ii $\forall \alpha, \beta \in \mathcal{A}_0, \mu(\alpha+\beta) = \mu(\alpha) + \mu(\beta)$

iii $\forall \alpha \in \mathcal{A}_0, \forall \lambda \in \mathbb{C}, \mu(\lambda\alpha) = \lambda\mu(\alpha)$ and more generally,

iv $\forall \alpha, \beta \in \mathcal{A}_0, \mu(\alpha\beta) = \mu(\alpha)\mu(\beta)$

Proofs:

i $\mathrm{Re}([x,x]) = \mathrm{Re}(x)$ and $\mathrm{Im}([x,x]) = \mathrm{Im}(x)$, hence the result.

ii $\forall \alpha, \beta \in \mathcal{A}_0, \mathrm{Re}(\alpha+\beta) = \mathrm{Re}(\alpha) + \mathrm{Re}(\beta)$

iii The result is obvious for $\lambda \in \mathbb{R}$. Moreover it is clear that $\mathrm{Im}(i\alpha) = \mathrm{Re}(\alpha)$ and similarly that $\mathrm{Re}(i\alpha) = -\mathrm{Im}(\alpha)$, thus

$$\begin{aligned}\mu(i\alpha) &= \frac{\min(-\mathrm{Im}\ \alpha) + \max(-\mathrm{Im}\ \alpha)}{2} + i\frac{\min(\mathrm{Re}\ \alpha) + \max(\mathrm{Re}\ \alpha)}{2} \\ &= \frac{(-\max(\mathrm{Im}\ \alpha)) + (-\min(\mathrm{Im}\ \alpha))}{2} + i\frac{\min(\mathrm{Re}\ \alpha) + \max(\mathrm{Re}\ \alpha)}{2} \\ &= -\mathrm{Im}(\mu(\alpha)) + i\mathrm{Re}(\mu(\alpha)) \\ &= i\mu(\alpha)\end{aligned}$$

Property ii enables us to conclude.

iv The case when α is a real interval is easy. Using property iii and the almost-ring structure of $\mathcal{A}_0$, the general case is proven. □

From these properties, it follows that μ is an almost-ring morphism.

For all $z \in \mathbb{C}$, let $\pm z = [-z, z]$ (obviously $\mu(\pm z) = 0$).

Theorem 1.2 (central decomposition)

$$\forall \alpha \in \mathcal{A}_0, \exists z \in \mathbb{C}, \{y \in \mathbb{C} / \alpha = \pm y + \mu(\alpha)\} = \{z, -z, \bar{z}, -\bar{z}\}$$

Proof. The existence on real intervals comes easily from the definition of μ. Now for $\alpha \in \mathcal{A}_0$, $\alpha = \mathrm{Re}(\alpha) + i\ \mathrm{Im}(\alpha)$, hence the existence of z such that $\{z, -z, \bar{z}, -\bar{z}\} \subset \{y \in \mathbb{C} / \alpha = \pm y + \mu(\alpha)\}$. The reciprocal inclusion comes from the fact that, for real numbers, it is true. □

Now let α^c be this centered interval $\alpha - \mu(\alpha)$, and $\mathcal{A}_0^c = \mathrm{Ker}(\mu)$ be the sub-almost-ring of centered intervals. Now that we defined the centered version of an interval, we can come back to computing $\alpha - \alpha$

$$\forall \alpha \in \mathcal{A}_0, \alpha - \alpha = 2(\alpha^c) = (2\alpha)^c$$

$$\alpha - \alpha = \mu(\alpha) + \alpha^c + (\mu(-\alpha) + (-\alpha)^c)$$

1.2.7 Magnitude

For all $\alpha \in \mathcal{A}_0$, we introduce $|\alpha| \in \mathbb{R}$ the *magnitude* of α

$$|\alpha| = \max\{|x|; x \in \alpha\}$$

Proposition 1.6 (magnitude from boundaries)

$$\forall x, y \in \mathbb{C}, |[x, y]| = \max(|x|, |y|)$$

Proof. Let $x, y \in \mathbb{C}$. $|x| \in \{|z|; z \in [x, y]\}$ so $|x| \leq |[x, y]|$ and $|y| \leq |[x, y]|$ thus $\max(|x|, |y|) \leq |[x, y]|$. Now let $z \in [x, y]$. $|\mathrm{Re}(z)| \leq \max(|\mathrm{Re}(x)|, |\mathrm{Re}(y)|)$ and equally for the imaginary part, hence $|z| \leq \max(|x|, |y|)$ by the triangular inequality, so $|[x, y]| \leq \max(|x|, |y|)$. □

1.3 Polar intervals

1.3.1 Definition

We have seen that cartesian complex intervals have interesting properties on sums while being harder to manipulate with products. Given the multiplicative nature of some of the structures we will define in the next chapter, is seems interesting to define a kind of complex interval that works better with products. Polar intervals were defined .

A polar complex interval is $\rho e^{i\theta}$ for $\rho, \theta \in \mathcal{A}_0^+$ (the product between ρ and $e^{i\theta}$ here is $\otimes$). The set of polar complex intervals is $\mathcal{S}_0$.

1.3.2 Operations

The most interesting property of polar complex intervals is the following.

Theorem 1.3 (directness of the product)
The product is direct in $\mathcal{S}_0$.

Proof. Let $\rho, \eta, \theta, \varphi \in \mathcal{A}_0^+$. By associativity and commutativity of $\otimes$,

$$\begin{aligned}
(\rho \otimes e^{i\theta}) \otimes (\eta \otimes e^{i\varphi}) &= (\rho\eta) \otimes e^{i\theta} \otimes e^{i\varphi} \\
&= \{re^{it}e^{ip}; r \in \rho \otimes \eta, t \in \theta, p \in \varphi\} \\
&= \{re^{i(t+p)}; r \in \rho \otimes \eta, t \in \theta, p \in \varphi\} \\
&= \{re^{i(t+p)}; r \in \rho \otimes \eta, x \in \theta \oplus \varphi\} \\
&= \{re^{i(t+p)}; r \in \rho\eta, x \in \theta + \varphi\} \\
&\qquad \text{(by directness of the sum and product in } \mathcal{A}_0^+) \\
&= \rho\eta e^{i(\theta+\varphi)} \in \mathcal{S}_0
\end{aligned}$$

□

Chapter 2

States & diagrams

2.1 Abstract states

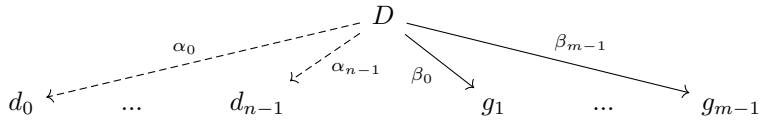
We now have intervals, *abstract elements* of $\mathbb{C}$ represented in $\mathcal{A}_0$. Our abstract elements for a n-qubit quantum state would be in $\mathcal{A}_n = {\mathcal{A}_0}^{2^n}$ for all $n \in \mathbb{N}$. Defining a sum in $\mathcal{A}_n$, and an external product $\alpha * A$ for $\alpha \in \mathcal{A}_0$ and $A \in \mathcal{A}_n$, comes easily. We also define the inclusion relation in $\mathcal{A}_n$ (which is an order relation) $\subset$ using the cartesian product of sets:

$$\forall A = (a_0, ..., a_{2^n-1})^T, B = (b_0, ..., b_{2^n-1})^T \in \mathcal{A}_n, A \subset B \iff a_0 \times ... \times a_{2^n-1} \subset b_0 \times ... \times b_{2^n-1}$$

Intuitively, if A and B are in $\mathcal{A}_n$ and $A \subset B$, the abstract state A is more *precise* than B.

2.2 Decision diagrams

We inductively define abstract additive quantum decision diagrams (AAQDDs), starting from zero-depth decision. The only zero-depth diagram is $\boxed{1}$. Let for every set E be the set of finite subsets of E: $\mathscr{P}_f(E) = \{A \subset E / |A| < \infty\}$. If the set $\mathcal{D}_n$ of diagrams of depth n is defined, $n+1$-depth diagrams can have a finite number of left children in $\mathcal{D}_n$ and a finite number of right children in $\mathcal{D}_n$, each being associated with an abstract amplitude in $\mathcal{A}_0$.



Defining $\mathcal{D}_{n+1} = \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n) \times \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n)$ thus comes naturally. Eventually, let $\mathcal{D} = \bigcup_{n \in \mathbb{N}} \mathcal{D}_n$ the set of all AAQDDs.

2.3 Sub-diagrams

Sub-diagrams (or nodes) of a diagram $D \in \mathcal{D}_n$ for all $n \in \mathbb{N}$, are defined inductively:

$$\mathcal{N}(\boxed{1}) = \boxed{1}$$

$$\forall D, G \in \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n), \mathcal{N}(D, G) = \{d; (\alpha, d) \in D \cup G\} \cup \bigcup_{(\alpha,d) \in D \cup G} \mathcal{N}(d)$$

We also define $\mathcal{N}_i(D) = \mathcal{N}(D) \cap \mathcal{D}_i$ for all $i \in \mathbb{N}$ the nodes "at height i".

2.4 Diagram evaluation

Now that we defined our decision diagrams, we can evaluate them to get abstract elements. We inductively define our evaluation function for n quibits $\mathcal{E}_n : \mathcal{D}_n \to \mathcal{A}_n$:

$$\mathcal{E}_0(\boxed{1}) = \{1\}$$

$$\forall D, G \in \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n), \mathcal{E}_{n+1}(D, G) = \begin{pmatrix} \sum\limits_{(\alpha,g)\in G} \alpha * \mathcal{E}_n(g) \\ \sum\limits_{(\beta,d)\in D} \beta * \mathcal{E}_n(d) \end{pmatrix} \quad \text{with}$$

Since there is no risk of ambiguity, defining $\mathcal{E} : \bigcup \mathcal{D}_n \to \bigcup \mathcal{A}_n$ is not problematic. With this last function, we can now evaluate all our AAQDDs and define a partial order $\leq$ on $\mathcal{D}$, with:

$$\forall A, B \in \mathcal{D}, A \leq B \iff \mathcal{E}(A) \subset \mathcal{E}(B)$$

Additionally, we extend the definition of the imprecision function $\mathcal{I}$ to diagrams: $\forall D \in \mathcal{D}, \mathcal{I}(D) = \mathcal{I}(\mathcal{E}(D))$. Note that $\forall A, B \in \mathcal{D}_n, A \leq B$ implies that $\mathcal{I}(A) \leq \mathcal{I}(B)$ but that the reciprocal is not generally true.

2.5 Error estimation

Let $A, C \in \mathcal{D}_n$. We would like to define a scale $\delta : \mathcal{D}_n \to X$ with $(X, \prec)$ a partially ordered set, that we would be able to compute in polynomial time and space (i.e. in $O(n^p)$ for a certain $p \in \mathbb{N}$), such that if $A \leq C$, $\delta(A) \prec \delta(C)$. Let $X = \mathcal{A}_0 \times \mathbb{R}^+$ and $\delta(A) = (\rho(A), \varepsilon(A))$ be inductively defined by:

$$\delta(\boxed{1}) = (\{1\}, \{0\})$$

$$\forall G, D \in \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n), \rho((G, D)) = \left(\sum_{(l,L)\in G} l\rho(L)\right) \bigsqcup \left(\sum_{(r,R)\in D} r\rho(R)\right)$$

$$\forall G, D \in \mathscr{P}_f(\mathcal{A}_0 \times \mathcal{D}_n), \varepsilon((G, D)) = \left(\sum_{(l,L)\in G} l \max|\rho(L) \ominus \varepsilon(L)| + \varepsilon(L)\right) \bigsqcup \left(\sum_{(r,R)\in D} r \max|\rho(R) \ominus \varepsilon(R)| + \varepsilon(R)\right)$$

with $\ominus$ the "crop" operation defined such that

$$\forall \alpha, \beta \in \mathcal{A}_0, (\alpha \ominus \beta) + \beta = \alpha$$

Proposition 2.1
The radius ρ of a diagram is bigger than all it's abstract amplitudes, i.e.

$$\forall n \in \mathbb{N}, \forall D \in \mathcal{D}_n \forall i \in \{0, ..., 2^n - 1\}, \mathcal{E}(A)[i] \subset \rho(A)$$

Proof. $\boxed{n=0}$ Let $d \in \mathcal{D}_0$, then $d = \boxed{1}$ hence the property since $\mathcal{E}(d)[0] = \rho(d) = \{1\}$
$\boxed{n>0}$ Let us assume that

$$\forall D \in \mathcal{D}_{n-1} \forall i \in \{0, ..., 2^{n-1}-1\}, \mathcal{E}(A)[i] \subset \rho(A)$$

Let $(G, D) \in \mathcal{D}_n$, then

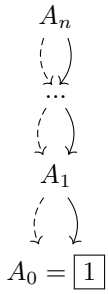
$$\rho((G,D)) = \left(\sum_{(l,L)\in G} l\rho(L)\right) \bigsqcup \left(\sum_{(r,R)\in D} r\rho(R)\right)$$

With usual operation properties on the sum and the join, we have the desired result. □

2.6 Non-additive diagrams

We can also define non-additive diagrams, which are diagrams that have at most one left child and one right child. We define $\mathcal{D}^* = \bigcup_{n\in\mathbb{N}} \mathcal{D}_n^*$ the set of all non-additive diagrams, with $\mathcal{D}_n^* = \mathscr{S}(\mathcal{A}_0 \times \mathcal{D}_{n-1}^*) \times \mathscr{S}(\mathcal{A}_0 \times \mathcal{D}_{n-1}^*)$ and $\mathscr{S}(E) = \{\{x\}; x \in E\} \cup \{\emptyset\}$. As we will see in the next chapter, non-additive diagrams have convenient properies that are not generally verified in additive diagrams, enabling us to provide a reduction algorithm.

Even more specifically, we define abstract chains as diagrams that have at most one left child and one right child, and if having two children, those two children being equal. We define $\mathcal{D}^\dagger = \bigcup_{n\in\mathbb{N}} \mathcal{D}_n^\dagger$ the set of all abstract chains, with $\mathcal{D}_n^\dagger$ the set of abstract chains of height n.



Chapter 3

Gate application

To use our diagrams in real-world cases, it is not only sufficient to be able to store them effectively, but also to be able to apply quantum gates on our states. Our first goal was to implement a short list of the most commonly used gates:

- 1-qubit gates: Pauli gates, Hadamard gate, rotation and phase gates
- 2-qubit gates: particularly CNOT and SWAP

3.1 Preliminary considerations

Let a diagram $D \in \mathcal{D}_m$ and a k-qubit gate P. We would like to apply P on the qubits $q = (q_1, ..., q_k)$ with $\forall i, 0 \leq q_i \leq m-1$ of D, and note the result $P_q(D)$.

The usual representation of P is a square matrix of size 2^k, which we can interprate as a matrix of elements of $\mathcal{A}_0$. When using this representation, applying P on D is equivalent to applying the matrix P on the vector $\mathcal{E}(D)$.

Obviously, we would like gate application on diagrams to follow gate application on matrices.

Definition 3.1 (valid gate application)
A gate application P_q is valid if and only if

$$\mathcal{E}(P_q(D)) = P_q \mathcal{E}(D)$$

In the case of consecutive qubits ($q_{i+1} = q_i + 1$), since in matrix form

$$P_q = \left(\bigotimes^{q_1 - 1} I \right) \otimes P \otimes \left(\bigotimes^{m-k-q_1-1} I \right)$$

we expect the application of P_q to be able to be performed "locally" on the diagram, i.e. without having to consider the whole diagram but only the qubits of q.

3.2 Single-qubit gates

3.2.1 X gate

The X gate is a Pauli gate that acts as a bit-flip on the qubit. It is represented by the following matrix:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

For a given diagram $D \in \mathcal{D}_m$, this gate can be applied to any qubit $0 \leq n \leq m-1$. We note the result $X_n D$. For the application to be valid, we expect

$$\mathcal{E}(X_n D) = X_n(\mathcal{E}(D))$$

Thus, we define the gate application as follows:

$$X_n(L,R) = \begin{cases} (R,L) & \text{if } n = 0 \\ (\{(a_l, X_{n-1})l; (a_l, l) \in L\}, \{(a_r, X_{n-1})r; (a_r, r) \in R\}) & \text{otherwise} \end{cases}$$

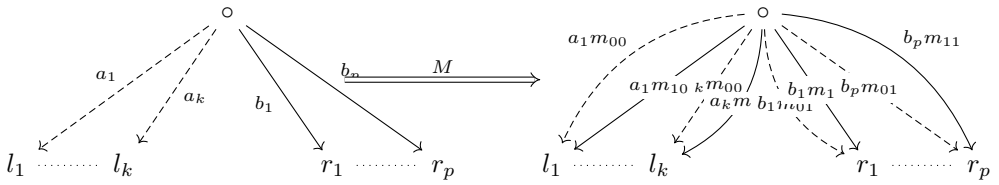
Visually, this corresponds to flipping the direction of all branches on level n.

3.2.2 General case

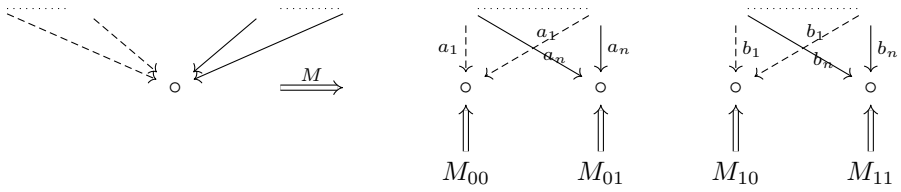
While intuitive, the above case cannot handle more complex 1-qubit gates, and notably the Hadamard gate. Let M be a matrix representing a 1-qubit quantum gate.

$$M = \begin{pmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{pmatrix}$$

The application of M on a qubit n of a diagram D is defined as follows:



3.3 2-qubit gates



Chapter 4

Reduction

4.1 Foundation

4.1.1 Approximations

We note that multiple QDDs can be evaluated to the same abstract state. This part will aim to provide an algorithm to decrease the "size" of diagrams while not breaking their evaluation by $\mathcal{E}$. The size of a AAQDD is the number of intervals (counting them with their multiplicity). We would want, from a diagram D, to get a diagram D' such that $\text{size}(D) > \text{size}(D')$ and $D \leq D'$ (the reduction is smaller in size and might be less precise than the original diagram). More generally, function $g : \mathcal{D}_n \to \mathcal{D}_n$ is an *global approximation* if

$$\forall D \in \mathcal{D}_n, D \leq g(D)$$

Similarly, a function $f : \mathcal{D}_n \times \mathcal{D}_n \to \mathcal{D}_n$ is a *merge approximation at height* n if

$$\begin{cases} \forall A \neq B \in \mathcal{D}_n, A \leq f(A,B) \text{ and } B \leq f(A,B) \\ \forall A \in \mathcal{D}_n, f(A,A) = A \end{cases}$$

We developed a reduction formula to force the merging of two nodes. This is permitted both thanks to abstract interpretation (to merge without amplitudes being colinear) and the additive nature of diagrams. The cost $\mathcal{C}_f : \mathcal{D}_n \to \mathbb{R}^+$ of applying a global approximation f to a diagram $D \in \mathcal{D}_n$ is defined by:

$$\mathcal{C}_f(D) = \mathcal{I}(f(D)) - \mathcal{I}(D)$$

4.1.2 Merging theorem

Let $n \in \mathbb{N}^*$, $N \geq n$, and f be a merge approximation. Moreover let $w : \mathcal{D}_N \to \mathcal{D}_n \times \mathcal{D}_n$ be a choice function at height n in $\mathcal{D}_N$, meaning that $\forall D, w(D) \in \mathcal{N}_n(D) \times \mathcal{N}_n(D)$. Now we define:

$$f|w : \left| \begin{array}{ccc} \mathcal{D}_N & \longrightarrow & \mathcal{D}_N \\ D & \longmapsto & r_N(B, C, r_N(A, C, D)) \quad \text{with } C = f(w(D)) \end{array} \right.$$

With $\forall i > 0, r_i : \mathcal{D}_n \times \mathcal{D}_n \times \mathcal{D}_i \to \mathcal{D}_i$ the replacement function defined by:

$$\begin{cases} \forall n > i, \forall A, B \in \mathcal{D}_n, \forall D \in \mathcal{D}_i, r_i(A, B, D) = D \\ \forall A, B, D \in \mathcal{D}_n, r_n(A, B, D) = \begin{cases} B & \text{if } D = A \\ D & \text{otherwise} \end{cases} \\ \forall 1 \leq n < i, \forall A, B \in \mathcal{D}_n, \forall \{(\alpha_j, g_j)\}, \{(\beta_k, d_k)\} \in \mathcal{D}_{i-1}, \\ \quad r_i(A, B, (G, D)) = (\{(\alpha_j, r_{i-1}(g_j))\}, \{(\beta_k, r_{i-1}(d_k))\}) \end{cases}$$

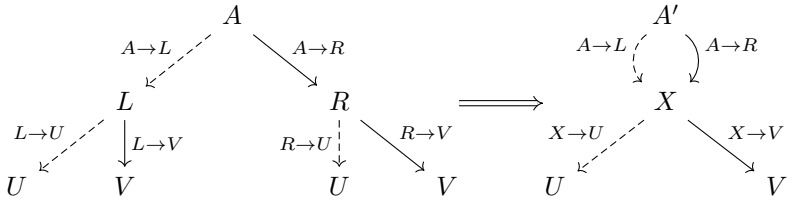
Merging theorem: Let f be a merge approximation at height n and w be a choice function at height n in $\mathcal{D}_N$. $f|w$ is a global approximation in $\mathcal{D}_N$.
Proof: Let $D \in \mathcal{D}_N$, $(A, B) = w(D)$ and $C = f(w(D))$. By ascending induction (in height), it comes that $\forall U, V \in \mathcal{D}_n, U \leq V \Rightarrow r_N(U, V, D) \leq D$. Meanwhile, f is a merge approximation so $A \leq C$, thus $r_N(A, C, D) \leq D$.

Proving that $r_N(A, C, D) \leq D$ is mostly enough to prove the theorem, because once it is proven we only have let $D' = r_N(A, C, D)$ and use this result on B and D' to conclude that $r_N(B, C, D') \leq D'$. The only problem is that we would need $C' = f(w(D'))$ instead of C to reuse the exact same result demonstrated earlier. □

4.2 Abstract quantum decision diagrams

Non-additive abstract quantum decision diagrams, because they only have at most one left child and one right child, are easier to manipulate than AAQDDs. In this section we show, given an AQDD A of height n and n integers $m_1, ..., m_n$ an algorithm to get an AQDD A' of height n such that $D \leq A'$ and that $\forall i \in \{0, ..., n\}, |\mathscr{N}_i(A')| \leq |\mathscr{N}_i(A)|$. This implies that size$(A)$ > size(A').

This algorithm relies on the following transofrmation, that allows us to merge two nodes.



with $X \to U = (L \to U) \sqcup (R \to U)$ and $X \to V = (L \to V) \sqcup (R \to V)$. With $X = f_m(L, R)$, such a defined function f_m is a merge approximation, which makes $A' = f(A, L, R)$ an approximation of A using the merging theorem.

Algorithm 1 Chaining of non-additive AQDDs

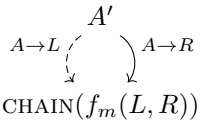
function CHAIN(A)
  $L \leftarrow$ left_child(A)
  $R \leftarrow$ right_child(A)
  if children(L) = children(R) **then**
    $A \leftarrow f(A, L, R)$
    child(A) $\leftarrow$ CHAIN(child(A))
  else ▷ We can do better by reducing one child and retrying to merge
    $L \leftarrow$ CHAIN(L)
    $R \leftarrow$ CHAIN(R)
    $A \leftarrow$ ZIP($f(A, L, R)$)
  end if
  return A
end function
function ZIP($n; k; L_k, ..., L_1; R_k, ..., R_1; X$)
  if $k = 0$ **then**
    return X
  else
    return ZIP($n; k; L_k, ..., L_2; R_k, ..., R_2; f_m(L_1, R_1)) + (X)$
  end if
end function

Theorem 4.1 (Chaining of non-additive AQDDs)

$$\forall n \in \mathbb{N}, \begin{cases} \text{CHAIN}(A) \textit{ is a chain} \\ \text{CHAIN}(A) \leq A \end{cases}$$

Proof. The proof is done by induction on the height of the AQDD A. The base case is trivial, as the AQDD is a leaf and the algorithm returns the same AQDD. Let us assume that the theorem holds for AQDDs of height $n-1$. We will show that it holds for AQDDs of height n.

Case 1: The children of A are the same. In this case A' is

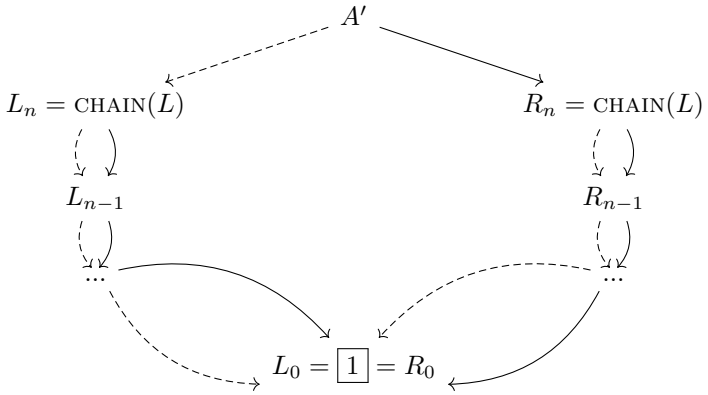


Since $f_m(L, R) \in \mathcal{D}_{n-1}$, by induction CHAIN($f_m(L, R)$) is a chain of AQDDs of height $n-1$. Additionally

$$\begin{cases} \text{CHAIN}(f_m(L, R)) \leq f_m(L, R) \leq L \\ \text{CHAIN}(f_m(L, R)) \leq f_m(L, R) \leq R \end{cases}$$

so $(A \to L)\text{CHAIN}(f_m(L, R)) \leq A \to L)L$ and $(A \to R)\text{CHAIN}(f_m(L, R)) \leq A \to R)R$.

Case 2: The children of A are different. In this case, we have that A' is



Now, just like closing a zipper, we will merge the AQDDs L_{n-1} and R_i to get A_i and then merge A_i with L_{i+1} and R_{i+1} to get A_{i+1}. We will repeat this process until we get $A_n = 1$. This process is guaranteed to terminate because the height of the AQDDs we are merging is increasing at each step and is lower than n.

□

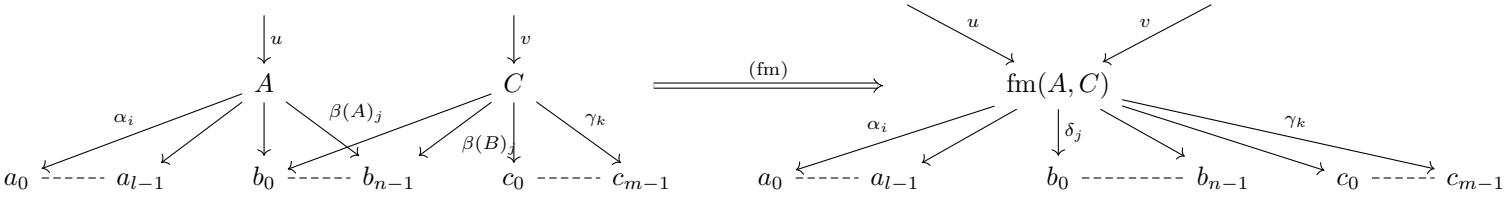
4.3 Abstract additive quantum decision diagrams

4.3.1 One-side case

To begin, let's consider the simple case where all diagrams only have left children (this case would be useless in practice because it would result in only one interval and zeros). Let's say we want to merge the two diagrams:

$$A = (\{(\alpha_0, a_0), ..., (\alpha_{l-1}, a_{l-1}), (\beta(A)_0, b_0), ..., (\beta(A)_{n-1}, b_{n-1})\}, \emptyset) \quad \text{and}$$
$$C = (\{(\beta(C)_0, b_0), ..., (\beta(C)_{n-1}, b_{n-1}), (\gamma_0, c_0), ..., (\gamma_m, c_{m-1})\}, \emptyset)$$

with $\{a_0, ..., a_{l-1}\} \cap \{c_0, ..., c_{m-1}\} = \emptyset$. A graphic representation of our merging formula would be:



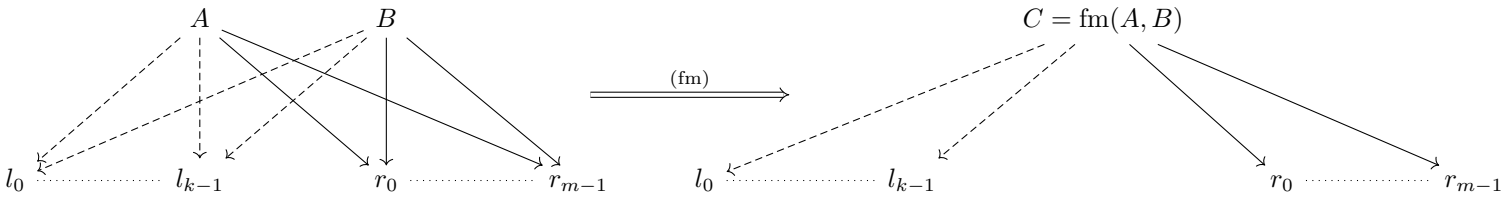
with $\delta_j = \beta(A)_j \sqcup \beta(B)_j$. More formally, the merging formula would be:

$$\text{fm}(A, C) = (\{(\alpha_0, a_0), ..., (\alpha_{l-1}, a_{l-1}), (\delta_0, b_0), ..., (\delta_{n-1}, b_{n-1}), (\gamma_0, c_0), ..., (\gamma_m, c_{m-1})\}, \emptyset)$$

4.3.2 Fully connected case

Let's consider another case, where our two nodes A and B have both a common left-descendance and a common right-descendance. We will see later that the general case can always be reduced

to this case. The abstract amplitude on the link between two nodes is $\text{ampl}(u, v)$, for example $\text{ampl}(A, l_0)$ or $\text{ampl}(B, l_0)$. Additionally, let $X = \{l_0, ..., l_{k-1}, r_0, ..., r_{m-1}\}$.



Where the new abstract amplitudes are defined by the following formula:

$$\forall x \in X, \text{ampl}(C, x) = \text{ampl}(A, x) \sqcup \text{ampl}(B, x)$$

Proof: Let $f : \mathcal{D}_n \times \mathcal{D}_n \to \mathcal{D}_n$ be our diagram transofrmation. Let $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathcal{A}_0$ such that $\alpha_0 \subset \beta_0$ and $\alpha_1 \subset \beta_1$.

$$\min(\min \text{Re}(\beta_0), \min \text{Re}(\beta_1)) \leq \min(\min \text{Re}(\alpha_0), \min \text{Re}(\alpha_1)) \qquad \text{and}$$
$$\max(\max \text{Re}(\beta_0), \max \text{Re}(\beta_1)) \geq \max(\max \text{Re}(\alpha_0), \max \text{Re}(\alpha_1))$$

thus $\text{Re}(\alpha_0 \sqcup \alpha_1) \subset \text{Re}(\beta_0 \sqcup \beta_1)$. The same goes for imaginary parts, hence $\alpha_0 \sqcup \alpha_1 \subset \beta_0 \sqcup \beta_1$. With a very similar proof, we can show that $\alpha_0 + \alpha_1 \subset \beta_0 + \beta_1$.

From there it comes that $\forall x \in X, \text{ampl}(A, x) \subset \text{ampl}(C, x)$ and $\forall x \in X, \text{ampl}(B, x) \subset \text{ampl}(C, x)$, and inductively:

$$\sum_{l \in \{l_0, ..., l_{k-1}\}} \text{ampl}(A, l) * l \subset \sum_{l \in \{l_0, ..., l_{k-1}\}} \text{ampl}(C, l) * l \qquad \text{and}$$
$$\sum_{r \in \{r_0, ..., r_{m-1}\}} \text{ampl}(A, r) * r \subset \sum_{r \in \{r_0, ..., r_{m-1}\}} \text{ampl}(C, r) * r$$

We now have $A \leq C$, and since A and B are interchangeable, $B \leq C$. Consequently, f is a merge approximation and according to the merging theorem, a global approximation can be derived from it. □