

# Contents

Acknowledgments . . . . .	4
Abstract . . . . .	5
Titre . . . . .	6
Résumé . . . . .	6
List of publications . . . . .	7
<b>1 Introduction</b>	<b>13</b>
<b>I Mathematical tools for quantum computation</b>	<b>19</b>
<b>2 Mathematical background</b>	<b>21</b>
2.1 Linear algebra . . . . .	21
2.1.1 Hilbert space . . . . .	21
2.1.2 Linear operator . . . . .	22
2.1.3 Gram matrix . . . . .	23
2.1.4 Norm, distance and fidelity . . . . .	23
2.2 Topology . . . . .	25
2.3 Analysis . . . . .	26
2.4 Probability theory . . . . .	27
2.5 Information theory . . . . .	28
2.6 Convexity, cones and order . . . . .	30
2.6.1 Preorder, infimum and supremum . . . . .	30
2.6.2 Cone and generalized inequality . . . . .	31
2.6.3 Separating and supporting hyperplane theorems . . . . .	31
2.6.4 Convex and concave function . . . . .	32
<b>3 Quantum mechanics and quantum computation</b>	<b>33</b>
3.1 Quantum mechanics . . . . .	33
3.1.1 Adiabatic quantum theorem . . . . .	34
3.2 Quantum computation . . . . .	37
<b>4 Query complexity</b>	<b>39</b>
4.0.1 Query complexity . . . . .	39
4.1 Quantum query complexity . . . . .	40
4.1.1 Discrete-time model . . . . .	41
4.1.2 Continuous-time model . . . . .	41
4.1.3 Output conditions . . . . .	43
4.2 Gram matrix representation . . . . .	44

4.3	Lower bound methods . . . . .	46
4.3.1	Polynomial method . . . . .	46
4.3.2	Adversary method . . . . .	47
4.3.3	Multiplicative adversary method . . . . .	49
<b>5</b>	<b>Communication complexity</b>	<b>53</b>
5.0.1	Communication model . . . . .	53
5.1	Lower bound methods . . . . .	55
5.1.1	Discrepancy . . . . .	56
5.1.2	Partition bound . . . . .	56
5.1.3	Information complexity . . . . .	58
5.2	Zero-communication model . . . . .	59
5.3	More lower bound methods . . . . .	62
5.4	Simulation model . . . . .	64
5.5	One-way model . . . . .	65
<b>6</b>	<b>Convex optimization</b>	<b>67</b>
6.1	Optimization problems . . . . .	67
6.2	Category of optimization problems . . . . .	68
6.3	Lagrangian and duality . . . . .	69
6.4	Lagrange dual function . . . . .	70
6.5	Strong duality . . . . .	71
6.6	KKT conditions . . . . .	72
6.7	Convex optimization problems . . . . .	73
6.8	Envelope theorem . . . . .	75
<b>II</b>	<b>Contributions</b>	<b>77</b>
<b>7</b>	<b>A universal adiabatic quantum query algorithm</b>	<b>79</b>
7.1	Adversary lower bound in the continuous-time model . . . . .	80
7.2	Adiabatic quantum query algorithm . . . . .	82
<b>8</b>	<b>A new lower bound for <math>Q^{ct}</math></b>	<b>89</b>
8.1	Feasible differentiable paths . . . . .	90
8.2	Adversary methods . . . . .	92
8.2.1	Adversary method $\text{Adv}^{ct}$ . . . . .	92
8.2.2	Multiplicative adversary method $\text{Madv}^{ct}$ . . . . .	93
8.2.3	Relation between adversary methods . . . . .	94
8.3	Adversary action $\text{Sadv}$ . . . . .	96
8.3.1	Definition of $\text{Sadv}$ . . . . .	96
8.3.2	Query Lagrangian and its properties . . . . .	98
8.3.3	Necessary conditions on $\text{Sadv}$ . . . . .	102
8.3.4	Relation with $\text{Adv}^{ct}$ and $\text{Madv}^{ct}$ . . . . .	105
<b>9</b>	<b>Lower bound for Information complexity</b>	<b>109</b>
9.1	Zero information complexity $\text{IC}_0$ . . . . .	110
9.2	Dualization of $\text{IC}_0$ . . . . .	113
9.3	$\text{IC}_0$ with a product input distribution . . . . .	116
9.4	Relaxed information cost $\overline{\text{IC}}_0$ . . . . .	118

<i>CONTENTS</i>	11
9.5 $IC_0^\rightarrow$ in the one-way model . . . . .	123
9.6 Application . . . . .	126
9.6.1 $IC_0^\rightarrow$ for CHSH correlations . . . . .	127
9.6.2 $\overline{IC}_0$ for CHSH correlations . . . . .	128
9.6.3 $IC_0$ for CHSH correlations . . . . .	129
<b>Conclusion</b>	<b>131</b>
<b>III Appendices</b>	<b>133</b>
<b>A Adiabatic theorem without a gap condition</b>	<b>135</b>
<b>B Slater's theorem</b>	<b>139</b>
<b>C Envelope theorem</b>	<b>143</b>
<b>D Euler-Lagrange equation</b>	<b>145</b>
<b>Bibliography</b>	<b>148</b>
<b>Notation</b>	<b>155</b>