

Contents

1	Introduction	1
1.1	Locally decodable codes	1
1.1.1	Hadamard code	2
1.1.2	A code based on polynomial interpolation	3
1.2	Private information retrieval schemes	4
1.2.1	A PIR scheme based on polynomial interpolation	5
1.3	The history of LDCs and PIR schemes	6
1.3.1	The first generation: interpolation	7
1.3.2	The second generation: recursion	8
1.3.3	The third generation: point removal	9
1.3.4	Lower bounds	12
1.4	Applications of LDCs and PIR schemes	13
1.4.1	Secure multiparty computation	13
1.4.2	Other models of private information retrieval	14
1.4.3	Average-case complexity	16
1.5	Organization of the book	16
1.6	Addendum	17
2	Locally decodable codes via the point removal method	19
2.1	Notation	19
2.2	Locally decodable codes	20
2.3	Binary LDCs via point removal	20
2.3.1	Regular intersecting families of sets	21
2.3.2	Basic construction	22
2.3.3	The main construction: point removal	24
2.4	General LDCs via point removal	26
2.5	Combinatorially nice subsets of \mathbb{F}_p^*	30
2.6	Algebraically nice subsets of \mathbb{F}_p^*	32
2.6.1	3-dependences between p -th roots: sufficient conditions	34
2.6.2	k -dependences between p -th roots: a sufficient condition	35
2.6.3	Summary	39

2.7	Results	39
2.7.1	Results for three-query binary codes	40
2.7.2	Results for general codes	41
2.8	Addendum	42
2.8.1	The code	44
3	Limitations of the point removal method	47
3.1	Attaining subexponential length requires a nice sequence	47
3.1.1	Point removal method	47
3.1.2	Point removal and bounds for $P(r^t - 1)$	48
3.1.3	Our results	48
3.2	A nice sequence yields short dependences between p -th roots	49
3.2.1	Algebraically nice subsets of \mathbb{F}_q^*	50
3.2.2	Combinatorially nice subsets of \mathbb{F}_q^*	53
3.2.3	Summary	55
3.3	k -dependences between p -th roots: a necessary condition	56
3.4	3-dependences between p -th roots: a necessary condition	57
3.5	Summary	58
3.6	Conclusions	59
3.7	Addendum	59
4	Private information retrieval	61
4.1	Preliminaries	61
4.2	From LDCs to PIR schemes	62
4.2.1	Upper bounds for three-server binary PIR schemes	64
4.2.2	Upper bounds for general PIR schemes	65
4.3	A combinatorial view of two-server PIR	66
4.3.1	Bilinear PIR	69
4.3.2	Group-based PIR	69
4.4	Complexity of bilinear group-based PIR	70
4.4.1	Algebraic preliminaries	70
4.4.2	Algebraic formulation	71
4.4.3	Low-dimensional principal ideals in group algebras	72
4.5	Summary of lower bounds for two-server PIR	73
4.6	Addendum	74
	References	75
	Index	81