

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Design, not Programming . . . . .	1
1.2	Value of Names . . . . .	2
1.3	Familiarity, not Mastery . . . . .	2
<b>I</b>	<b>Software Architecture</b>	<b>5</b>
<b>2</b>	<b>General Principles Toolbox</b>	<b>7</b>
2.1	Principle of Least Surprise (POLS) . . . . .	7
2.2	Principle of Single Responsibility (POSR) . . . . .	8
2.3	Principle of Simplicity (KISS) . . . . .	8
2.4	Principle of Single Source (DRY) . . . . .	8
2.5	Principle of Least Knowledge (POLK) . . . . .	8
<b>3</b>	<b>Type Toolbox</b>	<b>9</b>
3.1	Sets . . . . .	10
3.1.1	Comparisons . . . . .	10
3.1.1.1	Membership $\in$ . . . . .	10
3.1.1.2	Subset $\subset$ and $\subseteq$ . . . . .	10
3.1.1.3	Superset $\supset$ and $\supseteq$ . . . . .	11
3.1.1.4	Equality . . . . .	11
3.1.2	Operations . . . . .	11
3.1.2.1	Union $\cup$ . . . . .	11
3.1.2.2	Intersection $\cap$ . . . . .	11
3.1.2.3	Division $\setminus$ . . . . .	11
3.2	Type Conversions . . . . .	12
3.3	Subtype . . . . .	12
3.4	Bottom Type . . . . .	12
3.5	Unit Type . . . . .	12
3.6	Polymorphic Data Types . . . . .	13
3.6.1	Parametric polymorphism . . . . .	13
3.7	Algebraic Data Types . . . . .	13
3.7.1	Tuples . . . . .	13

3.7.2	Record . . . . .	13
3.7.3	Sum . . . . .	14
3.8	“Type Program” . . . . .	14
<b>4</b>	<b>Function Toolbox</b>	<b>15</b>
4.1	Operations with a single Function . . . . .	15
4.1.1	Domain / Range . . . . .	15
4.1.2	Operations with a single function of one variable . . . . .	15
4.1.2.1	Injective . . . . .	15
4.1.2.2	Surjective . . . . .	16
4.1.2.3	Bijjective - One-to-One Correspondence . . . . .	16
4.1.2.4	Idempotent . . . . .	16
4.1.2.5	Involutive . . . . .	16
4.1.3	Operations with a single function of two variables . . . . .	16
4.1.3.1	Abelian Group . . . . .	16
4.1.3.1.1	Monoid . . . . .	16
4.1.3.1.2	Commutative Property . . . . .	16
4.1.3.1.3	Inverse . . . . .	16
4.1.4	Recursion / Corecursion . . . . .	16
4.2	Operations with Multiple Functions . . . . .	16
4.2.1	Field . . . . .	16
4.2.1.1	Ring . . . . .	16
4.2.1.1.1	Distributive Property . . . . .	16
4.2.2	Coroutines . . . . .	17
<b>5</b>	<b>Higher-order Function Toolbox</b>	<b>19</b>
5.1	Sort . . . . .	19
5.2	Filter . . . . .	19
5.3	Map . . . . .	19
5.4	Reduce/Fold . . . . .	19
5.4.1	Left and Right Reduce/Fold . . . . .	19
5.4.2	Tree Reduce/Fold . . . . .	19
5.5	Cumulative Scan . . . . .	19
<b>6</b>	<b>Abstract Data Types Toolbox</b>	<b>21</b>
6.1	Iterator . . . . .	21
6.2	List . . . . .	21
6.3	Stack . . . . .	21
6.4	Queue . . . . .	21
6.4.1	Priority Queue / Heap . . . . .	22
6.5	Graph . . . . .	22
6.5.1	Weighted . . . . .	22
6.5.2	Directed . . . . .	22
6.5.2.1	Directed Acyclic Graph . . . . .	22
6.6	Tree . . . . .	22
6.7	Dictionary . . . . .	22

6.8	Set . . . . .	22
<b>7</b>	<b>Data Processing Toolbox</b>	<b>23</b>
7.1	Relational Algebra . . . . .	23
7.1.1	Operations . . . . .	23
7.1.1.1	$\pi$ (Project) . . . . .	23
7.1.1.2	$\sigma$ (Select) . . . . .	23
7.1.1.3	$\rho$ (Rename) . . . . .	23
7.1.2	Join . . . . .	23
7.1.2.1	$\bowtie$ (Natural Join) . . . . .	23
7.1.2.2	$\theta$ Equijoin . . . . .	23
7.1.2.3	$\triangleright$ (Antijoin) . . . . .	23
7.1.2.4	$\div$ (Division) . . . . .	23
7.1.2.5	$\bowtie, \times$ (Semijoin) . . . . .	23
7.2	Normal Form . . . . .	23
7.2.1	UNF - Unnormalized Form . . . . .	23
7.2.2	1 <sup>st</sup> - Atoms Only . . . . .	23
7.2.3	2 <sup>nd</sup> - No Partial Key Dependency . . . . .	23
7.2.4	3 <sup>rd</sup> - No Non-key Dependency . . . . .	23
<b>8</b>	<b>Warehousing</b>	<b>25</b>
8.1	Pivot . . . . .	25
8.2	OLAP - Online Analytical Processing . . . . .	25
8.2.1	OLAP Cube . . . . .	25
8.3	OLTP - Online Transaction Processing . . . . .	25
<b>9</b>	<b>Concurrency Toolbox</b>	<b>27</b>
9.1	ACID - Atomicity, Consistency, Isolation, Durability . . . . .	27
9.1.1	Atomicity . . . . .	27
9.1.2	Consistency . . . . .	27
9.1.3	Isolation . . . . .	27
9.1.4	Durability . . . . .	27
9.2	CAP - Consistency, Availability, Partition-tolerance . . . . .	27
9.2.1	Consistency . . . . .	27
9.2.2	Availability . . . . .	27
9.2.3	Partition-tolerance . . . . .	27
9.2.4	Trade Offs . . . . .	27
9.2.4.1	CA . . . . .	27
9.2.4.2	CP . . . . .	27
9.2.4.3	AP . . . . .	27
9.2.4.3.1	Eventual Consistency . . . . .	27
9.3	ACID2 - Associative, Commutative, Idempotent, Distributed . . . . .	28
9.4	CALM - Consistency As Logical Monotonicity . . . . .	28
9.4.1	LBEC - Lattice Based Eventual Consistency . . . . .	28
9.4.1.1	CRDT - Conflict Free Data Type . . . . .	28
9.4.2	Operational Transform . . . . .	28

9.5	Share Nothing . . . . .	28
<b>10</b>	<b>Numerical Methods</b>	<b>29</b>
10.1	Sequences . . . . .	29
10.1.1	Recursive . . . . .	29
10.2	Interpolation . . . . .	29
10.3	Error Analysis . . . . .	29
10.4	Mesh . . . . .	29
10.4.1	Adaptive Mesh . . . . .	29
10.5	Uses . . . . .	29
10.5.1	Integration . . . . .	29
10.5.2	Differentiation . . . . .	29
10.5.3	Differential Equation . . . . .	29
10.5.4	Interpolation . . . . .	29
<b>11</b>	<b>Randomness</b>	<b>31</b>
11.1	RNG - Random Number Generator . . . . .	31
11.1.1	TRNG - True Random Number Generator . . . . .	31
11.1.2	PRNG - Pseudo Random Number Generator . . . . .	31
11.1.2.1	LSFR - Linear Shift Feedback Register . . . . .	31
11.1.2.2	CSPRNG - Cryptographically secure pseudorandom Number Generator . . . . .	31
11.2	Distributions . . . . .	31
11.2.1	Uniform . . . . .	31
11.2.2	Gaussian/Normal . . . . .	31
11.2.2.0.1	Box-Muller Transform . . . . .	31
<b>12</b>	<b>Statistics</b>	<b>33</b>
12.1	Sampling . . . . .	33
12.1.1	From an unknown population . . . . .	33
12.1.1.1	Observations . . . . .	33
12.1.2	From a known population . . . . .	33
12.1.2.1	Poisson Sampling . . . . .	33
12.1.2.1.1	Bernoulli Sampling . . . . .	33
12.1.2.2	Simple Random Sampling . . . . .	33
12.1.2.3	Stratified Sampling . . . . .	33
12.1.2.4	Cluster Sampling . . . . .	33
12.1.3	Error . . . . .	33
12.1.3.1	Sampling Errors and Biases . . . . .	33
12.1.3.1.1	Selection bias . . . . .	33
12.1.3.1.2	Random sampling error . . . . .	33
12.1.3.2	Non-sampling error . . . . .	33
12.1.3.2.1	Over-coverage . . . . .	33
12.1.3.2.2	Under-coverage . . . . .	33
12.1.3.2.3	Measurement Error . . . . .	33
12.1.3.2.4	Processing Error . . . . .	34

12.1.3.2.5	Non-response . . . . .	34
12.2	Summary Statistics . . . . .	34
12.2.1	Cardinality . . . . .	34
12.2.2	Total . . . . .	34
12.2.3	Moments . . . . .	34
12.2.3.1	1 <sup>st</sup> : Mean $\mu$ . . . . .	34
12.2.3.2	2 <sup>nd</sup> : Variance $\sigma^2$ or $Var(X)$ . . . . .	34
12.2.3.2.1	Standard Deviation $\sigma$ . . . . .	34
12.2.3.3	3 <sup>rd</sup> : Skew . . . . .	35
12.2.3.4	4 <sup>th</sup> : Kurtosis . . . . .	35
12.2.4	Mode . . . . .	35
12.2.5	Quantiles . . . . .	35
12.2.5.1	Median . . . . .	35
12.3	Modality . . . . .	35
12.3.1	Monomodal Distributions . . . . .	35
12.3.2	Multimodal Distributions . . . . .	35
12.4	Discrete Distributions . . . . .	35
12.4.1	Binomial Distribution . . . . .	35
12.4.1.1	Definition . . . . .	35
12.4.1.2	Usage . . . . .	35
12.4.2	Poisson distribution . . . . .	35
12.4.2.1	Definition . . . . .	35
12.4.2.2	Usage . . . . .	35
12.5	Continuous Distributions . . . . .	35
12.5.1	Gaussian / Normal . . . . .	35
12.5.1.1	Definition . . . . .	35
12.5.1.2	Usage . . . . .	35
12.5.1.3	Z-Score vs Probability . . . . .	35
12.5.2	$\chi^2$ Distribution . . . . .	35
12.5.2.1	Definition . . . . .	35
12.5.2.2	Usage . . . . .	35
12.5.3	Student's t Distribution . . . . .	35
12.5.3.1	Definition . . . . .	35
12.5.3.2	Usage . . . . .	35
12.5.4	Pareto Distribution . . . . .	35
12.5.4.1	Definition . . . . .	35
12.5.4.2	Usage . . . . .	35
<b>13</b>	<b>Cryptography</b> . . . . .	<b>37</b>
13.1	Key Management Concerns . . . . .	38
13.1.1	Physical security . . . . .	38
13.1.2	Logical security . . . . .	38
13.1.3	Personnel security . . . . .	38
13.2	Kerckhoffs' Principle / Shannon's Maxim . . . . .	38
13.3	Threat Model . . . . .	39
13.4	Cryptanalysis . . . . .	39

13.4.1	Brute Force . . . . .	39
13.4.1.0.1	Examples . . . . .	39
13.4.2	Known-plaintext . . . . .	39
13.4.2.0.1	Example . . . . .	39
13.4.2.1	Chosen-plaintext . . . . .	40
13.4.2.1.1	Example . . . . .	40
13.4.3	Side-Channel Attack . . . . .	40
13.4.3.1	Timing Attack . . . . .	40
13.4.3.2	Power-monitoring Attack . . . . .	40
13.4.3.3	Differential Fault Analysis . . . . .	40
13.4.4	System Attacks . . . . .	40
13.4.4.1	Man-in-the-Middle . . . . .	40
13.4.4.1.1	Downgrade Attack . . . . .	40
13.4.4.1.2	Examples . . . . .	40
13.4.4.2	Input Validation . . . . .	41
13.4.4.2.1	Examples . . . . .	41
13.4.4.2.2	Examples . . . . .	41
13.5	Message Digest / Hashing . . . . .	41
13.5.1	Attacks . . . . .	41
13.5.1.1	Collision Attack . . . . .	41
13.5.1.1.1	Rainbow Table . . . . .	41
13.5.1.2	Chosen-prefix Collision Attack . . . . .	41
13.5.1.3	Length Extension Attack . . . . .	41
13.5.2	HMAC - Keyed Hash Message Authentication Code . . . . .	41
13.6	PBKDF - Password Based Key Derivation Function . . . . .	41
13.6.1	PBKDF2 . . . . .	41
13.6.2	scrypt . . . . .	41
13.7	Password Storage . . . . .	41
13.8	Symmetric Encryption . . . . .	42
13.8.1	Stream Ciphers . . . . .	42
13.8.2	Block Ciphers . . . . .	42
13.8.2.1	Initialization Vectors . . . . .	42
13.8.2.2	Modes . . . . .	42
13.8.2.2.1	CBC - Cipher Block Chaining Mode . . . . .	42
13.8.2.2.2	CFB - Cipher Feedback Mode . . . . .	42
13.8.2.2.3	OFB - Output Feedback Mode . . . . .	42
13.8.2.2.4	CTR - Counter Mode . . . . .	42
13.8.2.2.5	GCM - Galois/Counter Mode (Authenticated) . . . . .	42
13.8.2.3	Authentication . . . . .	42
13.9	Asymmetric Encryption . . . . .	43
13.9.1	Operations . . . . .	43
13.9.1.1	Key Agreement . . . . .	43
13.9.1.2	Encryption / Decryption . . . . .	43
13.9.1.3	Sign / Verify . . . . .	43
13.9.2	Diffie-Hellman . . . . .	43

13.9.3	RSA	43
13.9.4	Elliptic Curves	43
13.9.4.1	ECDSA - Elliptic Curve Digital Signature Algorithm	43
13.9.4.2	EdDSA - Edwards-curve Digital Signature Algorithm	43
13.9.4.3	ECC - Elliptic Curve Cryptography	43
13.10	PKI - Public Key Infrastructure	43
13.10.1	Certificates	43
13.10.1.1	CA - Certificate Authorities	43

## II Software Engineering - Data Structures 45

<b>14</b>	<b>Run-time Analysis Toolbox</b>	<b>47</b>
14.1	Executive Summary	47
14.2	Real Analysis	47
14.2.1	Series	47
14.2.2	Convergence	47
14.2.3	Limits	47
14.3	Run-Time Analysis	47
14.3.1	RAM (Random Access Machine) Model	47
14.3.2	Rational / Justification	47
14.3.3	Examples	47
14.4	Measures	47
14.4.1	Big-O	47
14.4.2	Big- $\Theta$	47
14.4.3	Big- $\Omega$	47
<b>15</b>	<b>Abstract Data Structures Implementation Toolbox</b>	<b>49</b>
15.1	List	50
15.1.1	Array	50
15.1.2	Linked List	50
15.1.2.1	Singly Linked List	50
15.1.2.2	Doubly Linked List	50
15.1.3	Circular List/Buffer	50
15.2	Stack	50
15.2.1	List	50
15.3	Queue	50
15.3.1	List	50
15.4	Priority Queue	50
15.4.1	Heap	50
15.5	Iterator	50
15.6	Graph	50
15.6.1	Adjacency List	50
15.6.2	Adjacency Matrix	50

15.7	Tree	50
15.7.1	Binary Search Tree	50
15.7.2	Red-Black Tree	50
15.7.3	b-tree	50
15.8	Dictionary	50
15.8.1	Dual List	50
15.8.2	Hash Table	50
15.9	Set	50
15.9.1	Dictionary	50
15.9.2	Trie	50
15.9.3	Bloom Filter	50
15.9.3.1	Dual Bloom Filter	50
15.9.3.2	Counting Bloom Filter	50
<b>16</b>	<b>Abstract Data Structures Algorithms Toolbox</b>	<b>51</b>
16.1	Lists	51
16.1.1	Measures	51
16.1.1.1	Online Exact Calculations	51
16.1.1.1.1	Min/Max	51
16.1.1.1.2	Cardinality	51
16.1.1.1.3	Mean	51
16.1.1.1.4	Variance / Standard Deviation	51
16.1.1.2	Online Estimation Algorithms	51
16.1.1.2.1	Quantiles	51
16.1.2	Sorting	52
16.1.2.1	Bubble Sort (Swap)	52
16.1.2.2	Selection Sort (Select and Swap)	52
16.1.2.3	Insertion Sort (Select and Move)	52
16.1.2.4	Radix Sort (Bucket)	52
16.1.2.5	Heap Sort ()	52
16.1.2.6	Quicksort (Swap / Divide and Conquer)	52
16.1.2.7	Merge Sort (Merge / Divide and Conquer)	52
16.1.2.8	Tim Sort (Hybrid)	52
16.1.3	Searching	52
16.1.3.1	Naïve	52
16.1.3.2	Binary Search	52
16.1.4	Matching	52
16.1.4.1	Rabin-Karp	52
16.1.4.2	Knuth-Morris-Pratt	52
16.1.4.3	Boyer-Moore	52
16.1.5	Error Detection	52
16.1.5.1	Even/Odd Parity	52
16.1.5.2	CRC - Cyclic Redundancy Check	52
16.1.6	Error Correction	52
16.1.6.1	XOR Parity	52
16.1.6.2	Erasur Codes	52



16.2	Trees and Graphs . . . . .	52
16.2.1	Traversal . . . . .	52
16.2.1.1	DFS - Depth First Search . . . . .	52
16.2.1.2	BFS - Breath First Search . . . . .	52
16.2.1.3	Topological Sort . . . . .	52
16.2.2	Minimum Spanning Tree . . . . .	52
16.2.2.1	Prim's Algorithm . . . . .	52
16.2.3	Pathfinding . . . . .	52
16.2.3.1	Bellman-Ford algorithm . . . . .	52
16.2.3.2	Dijkstra's Algorithm . . . . .	52
16.2.3.3	A* . . . . .	52
16.2.4	Network Flow . . . . .	52
16.2.4.1	Edmonds-Karp algorithm . . . . .	52
16.2.4.2	MPM - Malhotra, Pramodh-Kumar, Maheshwari . . . . .	52
16.2.4.3	J. Orlin . . . . .	52
16.3	Sets . . . . .	52
16.3.1	Measures . . . . .	52
16.3.1.1	Online Estimation Algorithms . . . . .	52
16.3.1.1.1	Cardinality . . . . .	52

### III Software Engineering - Systems 55

<b>17</b>	<b>Concurrency Toolbox</b>	<b>57</b>
17.1	SQL Transaction Isolation Levels . . . . .	57
17.1.1	Read uncommitted . . . . .	57
17.1.2	Read committed . . . . .	57
17.1.3	Repeatable read . . . . .	57
17.1.4	Serializable . . . . .	57
17.2	CALM - Consistency as Logical Monotonicity . . . . .	57
17.2.1	Lattice-Based Eventual Consistency . . . . .	57
17.2.1.1	CRDT - Conflict-free Replicated Data Types . . . . .	57
17.2.1.1.1	G- and PN-Counter . . . . .	57
17.2.1.1.2	G- and 2P-Set . . . . .	57
17.2.1.1.3	LWW - Last Write Wins . . . . .	57
17.2.1.1.4	Sequence CRDTs . . . . .	57
17.2.1.2	Operational Transforms . . . . .	58
17.3	Share Nothing . . . . .	58
17.3.1	Message Passing . . . . .	58
17.4	Consensus . . . . .	58
17.4.1	Paxos . . . . .	58
17.4.1.1	MultiPaxos . . . . .	58
17.4.2	Raft . . . . .	58
17.4.3	Blockchain / Proof-of-Work . . . . .	58
17.5	Atomics . . . . .	58
17.6	Semaphores, Locks, and Mutexes (Oh My!) . . . . .	58

17.7 Non-Blocking Data Structures . . . . .	58
17.7.1 Lock-Free Data Structures . . . . .	58
17.7.1.1 Wait-Free Data Structures . . . . .	58
17.8 Transactional Memory . . . . .	58
<b>IV Software Engineering - Numeric Quantities</b>	<b>59</b>
<b>18 Representation</b>	<b>61</b>
18.1 Integer . . . . .	61
18.1.1 Unsigned . . . . .	61
18.1.2 2's Complement Signed . . . . .	61
18.2 Decimal . . . . .	61
18.2.1 Fixed Point . . . . .	61
18.2.2 Floating Point . . . . .	61
<b>19 Randomness</b>	<b>63</b>
19.1 PRNG - Pseudo Random Number Generator . . . . .	63
19.2 Distributions . . . . .	63
19.2.1 Uniform . . . . .	63
19.2.2 Gaussian/Normal . . . . .	63
<b>20 Error Analysis</b>	<b>65</b>
<b>21 Numerical Methods</b>	<b>67</b>
21.1 Integration . . . . .	67
21.1.1 Riemann Sum . . . . .	67
21.1.2 Trapezoidal Rule . . . . .	67
21.2 Differentiation . . . . .	67
21.2.1 Finite Difference . . . . .	67
21.3 Differential Equation . . . . .	67
21.3.1 Euler method . . . . .	67
21.3.2 Runge-Kutta . . . . .	67
21.4 Regression / Interpolation . . . . .	67
21.4.1 Least Squares . . . . .	67
21.4.2 Spline . . . . .	67