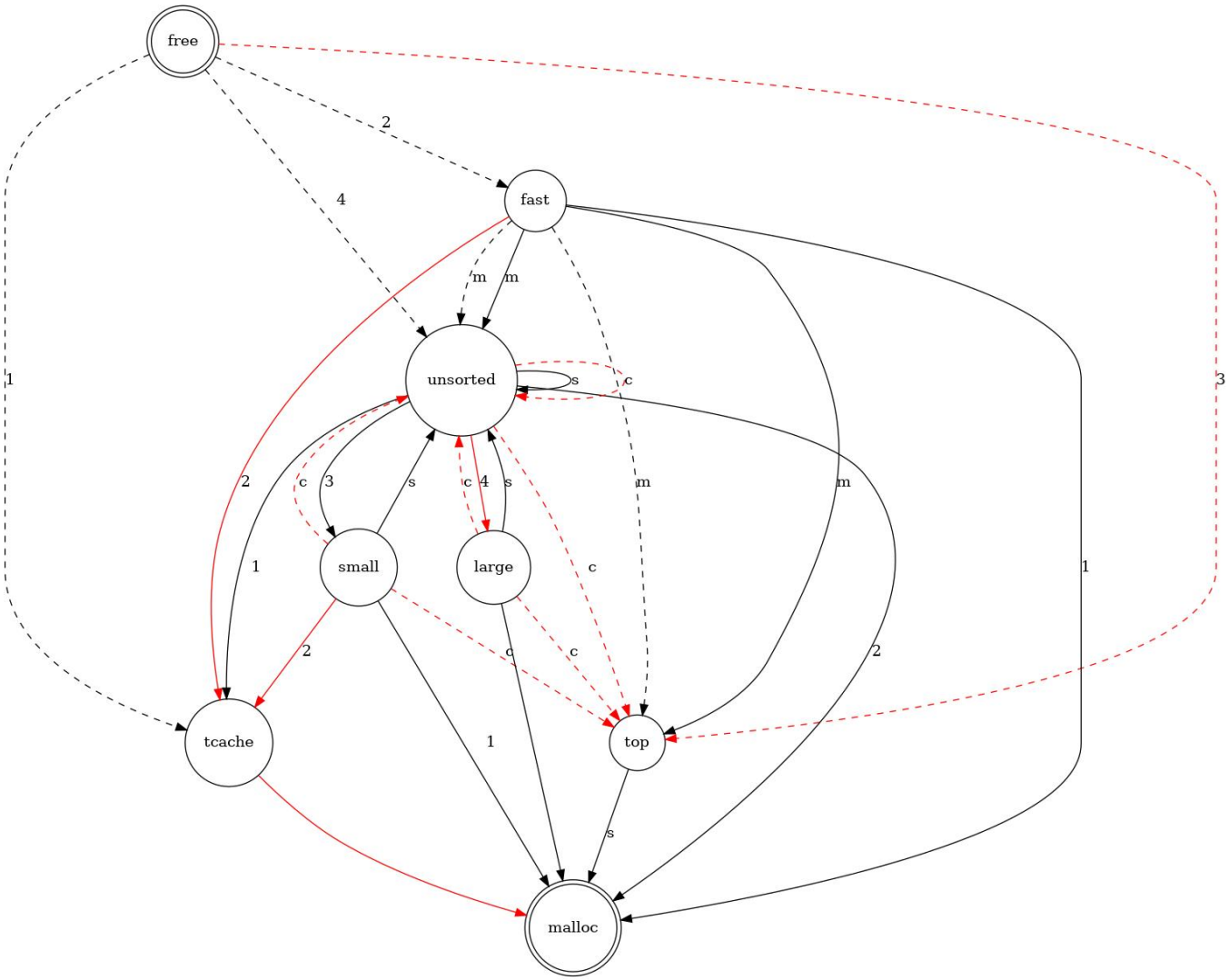
Heap Cheat Sheet

Transition



symbol	description
arrow	malloc
dotted arrow	free
red arrow	weak path
c	(for | back)word consolidate
m	malloc consolidate
s	split the chunk
0 ~ 4	priority (0: high, 4: low)

path	method	description
fast → malloc	malloc	1st chunk in fast bin when tcache is empty

path	method	description
fast → tcache	malloc	2nd ~ 8th chunks in fast bin when tcache is empty
unsorted → tcache	malloc	1st ~ 7th just-fit chunks in unsorted bin when tcache is empty
unsorted → malloc	malloc	8th just-fit chunk in unsorted bin when tcache is empty
small → malloc	malloc	1st chunk in small bin when tcache is empty
small → tcache	malloc	2nd ~ 8th chunks in unsorted bin when tcache is empty

Bins

	size	type
tcache	0x20 ~ 0x410	FILO
fast	0x20 ~ 0x80	FILO
unsorted	0x20 ~	FIFO
small	0x20 ~ 0x3f0	FIFO
large	0x400 ~	FIFO

Double Free

1st \ nth	tcahe	fast	unsorted
tcache	X	X	X
fastbin	O	O	-
unsorted [0x20 ~ 0x80]	O	O	X
unsorted [0x90 ~ 0x410]	O	-	X
unsorted [0x420 ~]	-	-	X
smallbin [0x20 ~ 0x80]	O	O	X
smallbin [0x90 ~ 0x3f0]	O	-	X
largebin [0x400, 0x410]	O	-	X
largebin [0x420 ~]	-	-	X