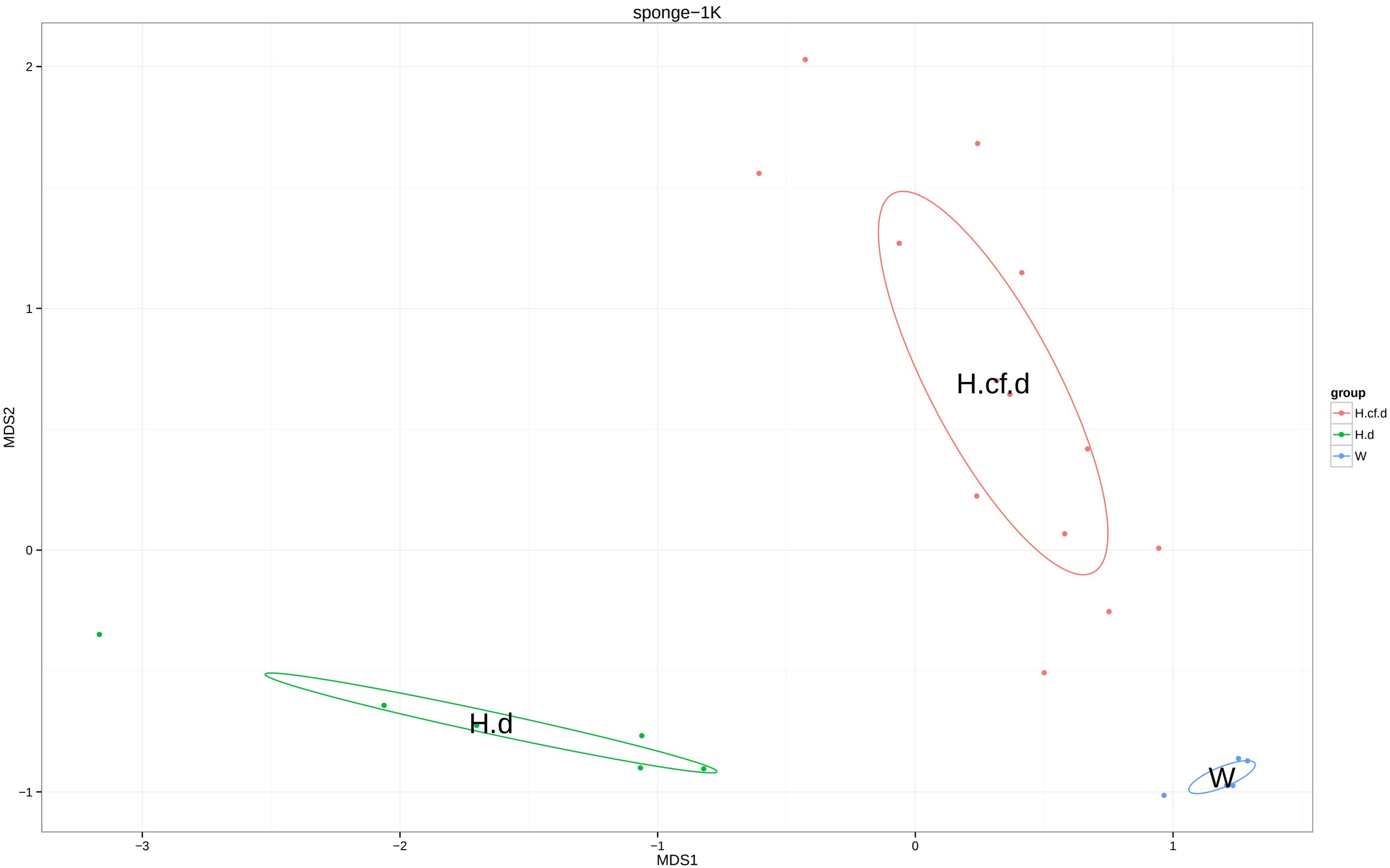
sponge−1K
MDS2
MDS1
2
1
0
−1
−3
−2
−1
0
1
H.cf.d
H.d
W
group
H.cf.d
H.d
W