

GCM (naive)