GNSS Signal Simulator

What is a GNSS signal simulator?

- GNSS signal simulators are radio frequency generating instruments that are capable of transmitting the same exact signals as GNSS satellites.
- GNSS signal simulators offer the most flexibility, compared to testing with over-the-air signals, or record and replay solutions.
- Without a simulator, attempts to test receiver with over-the-air signals would be limited to the satellites available at a particular time and place.

Advantage of Simulation

- Signal effects such as atmospheric disturbances, multipath and obscuration are quantified, controlled and precisely repeatable.
- Vehicle and satellite trajectory and associated dynamics are modelled.
- Future signals can be generated to allow testing against new signal before a complete constellation of satellites are transmitting the signal in space.

Quadrature Modulation

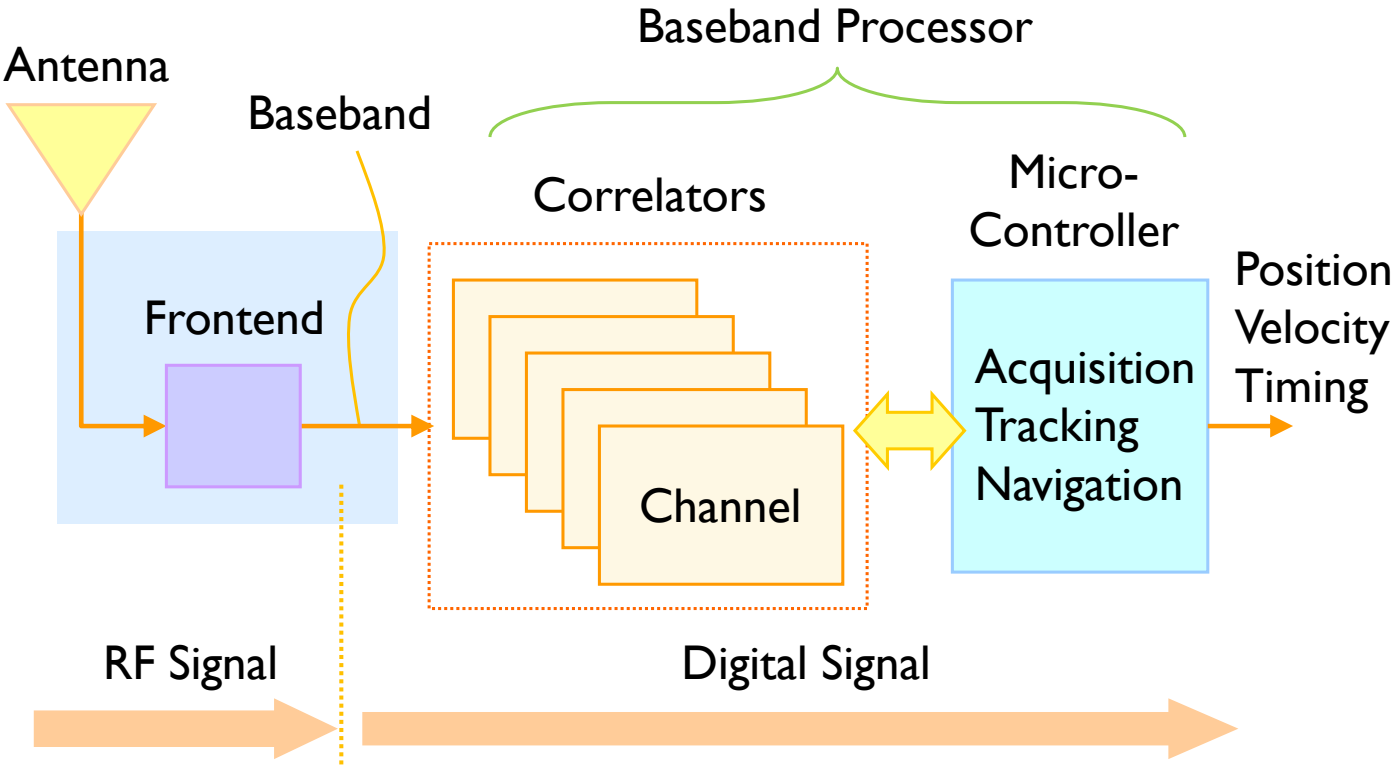
- Any phase shift keying can be generated by changing the amplitudes of two carrier waves.
- The two carrier waves of the same frequency are out of phase with each other by $90°$, a condition known as orthogonality or quadrature.

$$s(t) = \underbrace{\cos(\omega t}_{\text{Carrier Wave}} \underbrace{- \phi)}_{\text{Phase Keying}}$$

$$= \cos(\phi)\cos(\omega t) + \sin(\phi)\sin(\omega t)$$

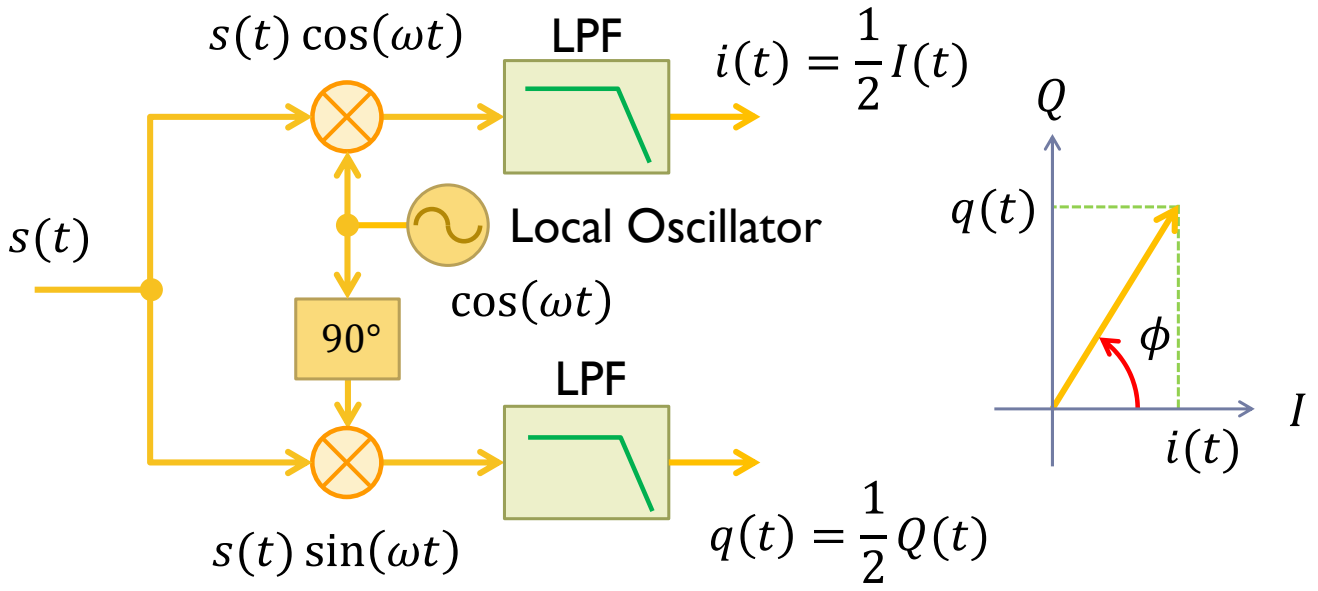
$$= \underbrace{I(t)}_{\text{In-phase}}\cos(\omega t) + \underbrace{Q(t)}_{\text{Quadrature}}\sin(\omega t)$$

GNSS Receiver Architecture



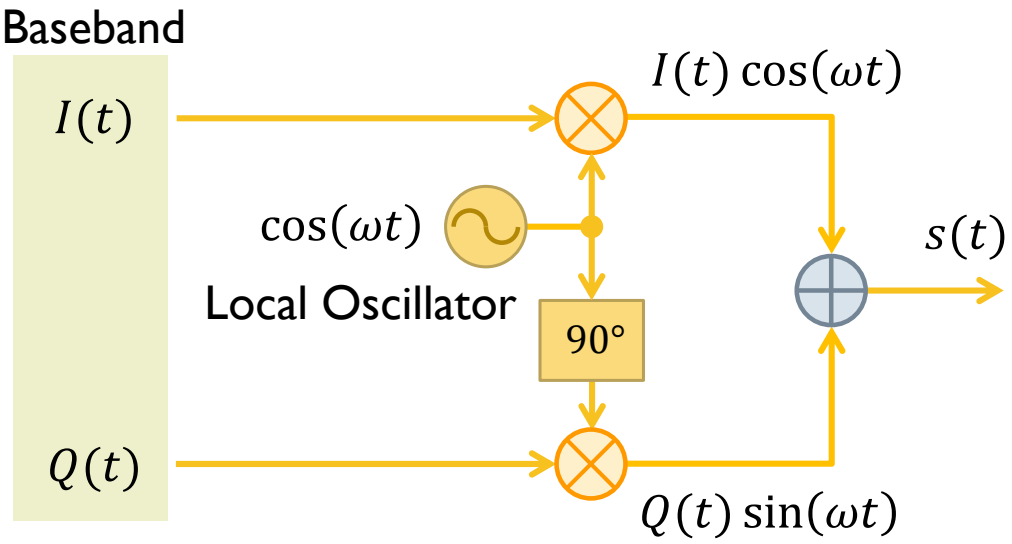
Coherent Demodulator

$$s(t) = I(t)\cos(\omega t) + Q(t)\sin(\omega t)$$



Record and Replay

- The premise of "record and replay" is to capture GNSS baseband signals off the air with an RF frontend and then replay them to a receiver with a quadrature modulator.



GNSS Baseband Signal Generation

- GNSS baseband signals can be generated numerically.
- GNSS receivers compare the received signal against a locally generated replica of the same code and carrier phase to identify which satellite has generated the corresponding signal.
  - The locally generated replica is identical to the incoming baseband signal.
- All the information about the civil GNSS signals are freely available to the public.

Software Defined Radio

- Software defined radio (SDR) is a radio communication system where components that have been traditionally implemented in hardware are instead implemented by means of software on a personal compute.
- Many SDR devices provide programmable radio platforms by combining an RF-to-baseband transceiver physical layer and a USB connection to the PC.

SDR Devices

	HackRF One	USRP B210	BladeRF x40	LimeSDR
Frequency Range	1MHz – 6GHz	70MHz – 6GHz	300MHz – 3.8GHz	100kHz – 3.8GHz
RF Bandwidth	20MHz	61.44MHz	40MHz	61.44MHz
Sample Depth	8-bit	12-bit	12-bit	12-bit
Sample Rate	20Msps	61.44Msps	40Msps	61.44Msps
TX/RX Channels	1/1	2/2	1/1	2/2
Interface	USB 2.0	USB 3.0	USB 3.0	USB 3.0
Price	$299	$1,119	$420	$299

Open-Source GPS Signal Simulator

- GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using SDR devices.
  - https://github.com/osqzss/gps-sdr-sim
- A user-defined trajectory can be specified in either a CSV file, which contains the Earth-centered Earth-fixed (ECEF) user positions, or an NMEA GGA stream.
- The GPS satellite constellation is specified through a GPS broadcast ephemeris file.
- These files are used to compute the range and Doppler of the GPS satellites in view. This range data is then use to generate the digitized I/Q samples for the GPS signal.

Real-Time GPS Signal Simulator

- Some real-time implementations of GPS-SDR-SIM for specific SDR devices are also available.
  - https://github.com/osqzss/bladeGPS (BladeRF)
  - https://github.com/osqzss/LimeGPS (LimeSDR)
  - https://github.com/Mictronics/multi-sdr-gps-sim (HackRF)
- Host PC requirements
  - Windows / Linux
  - Intel Core i5 @ 2.5GHz
  - 8GB RAM

Demonstration