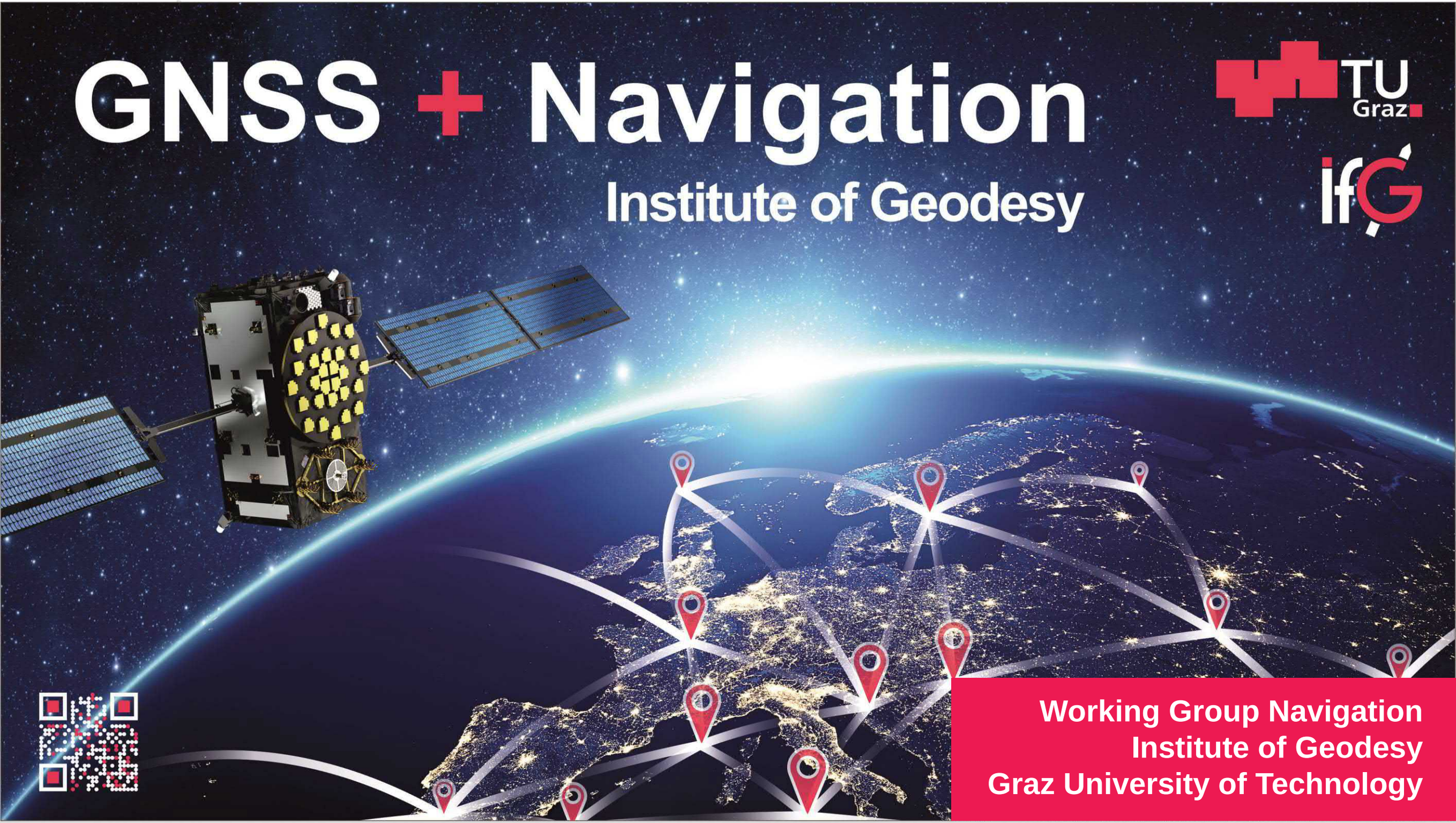
GNSS + Navigation

Institute of Geodesy



Working Group Navigation
Institute of Geodesy
Graz University of Technology

WISSEN
TECHNIK
LEIDENSCHAFT

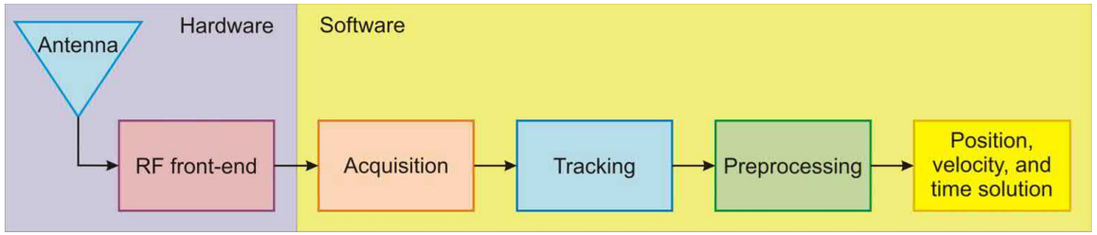
GNSS Signal Tracking

GNSS Under Attack Workshop - Ph. Berglez

6 February 2026

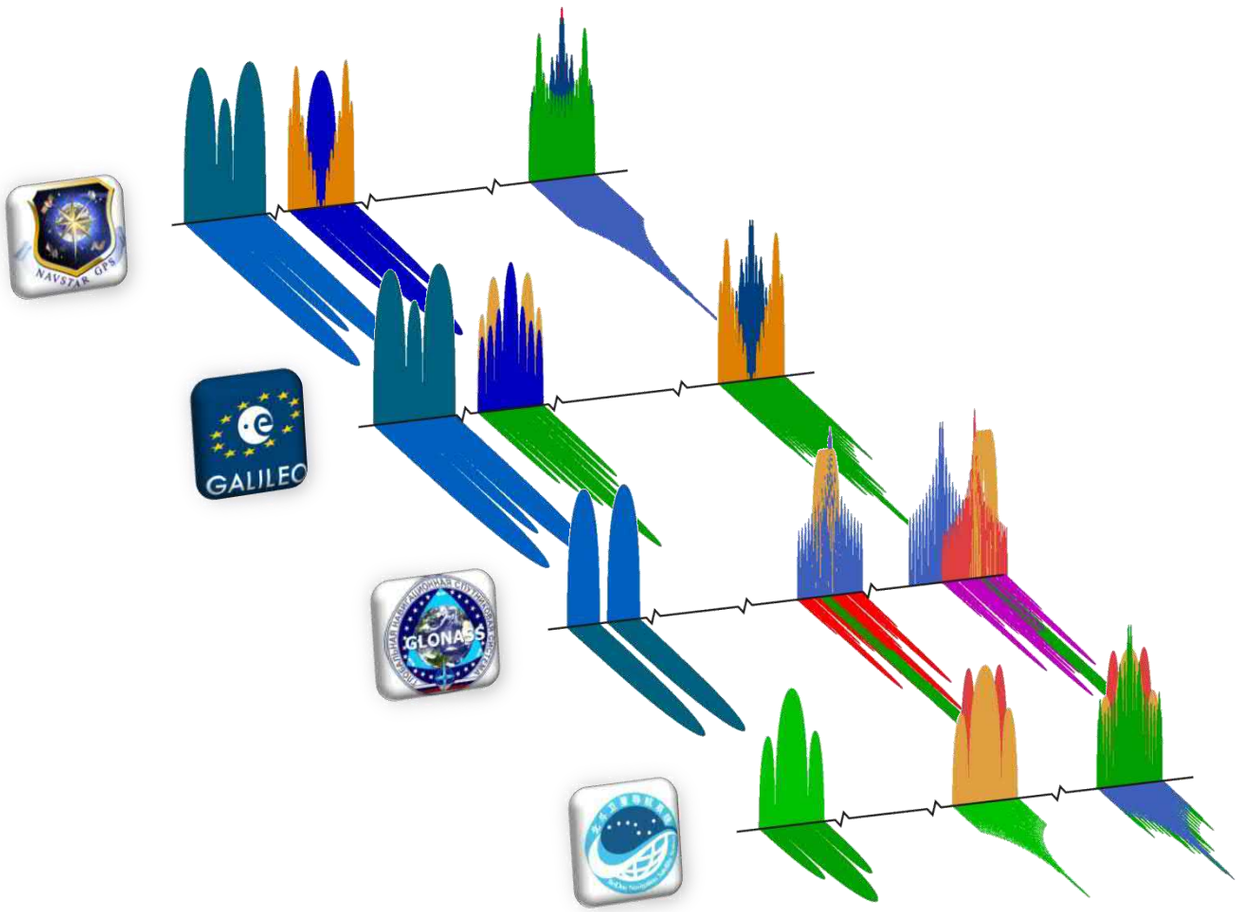
Objectives

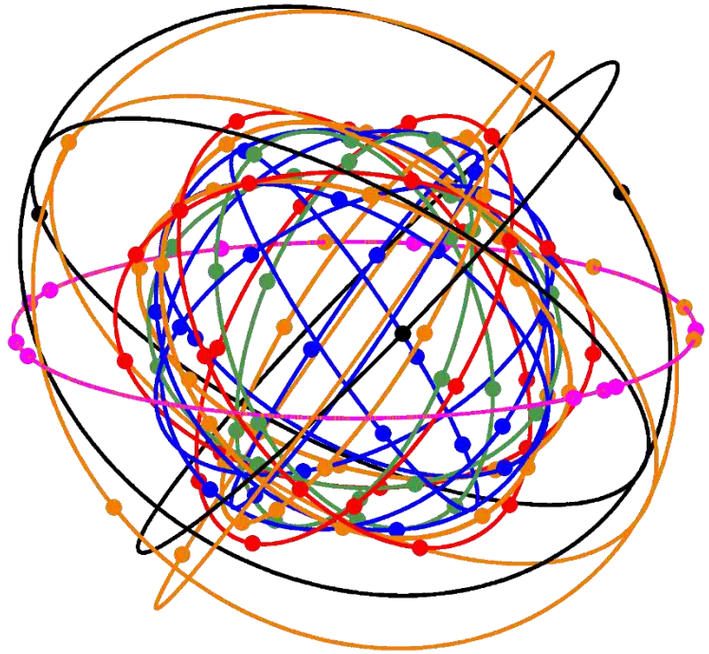
- Fundamentals of GNSS signal structure
- GNSS receiver - signal processing
- GNSS signal tracking



Fundamentals of GNSS signal structure

GNSS today



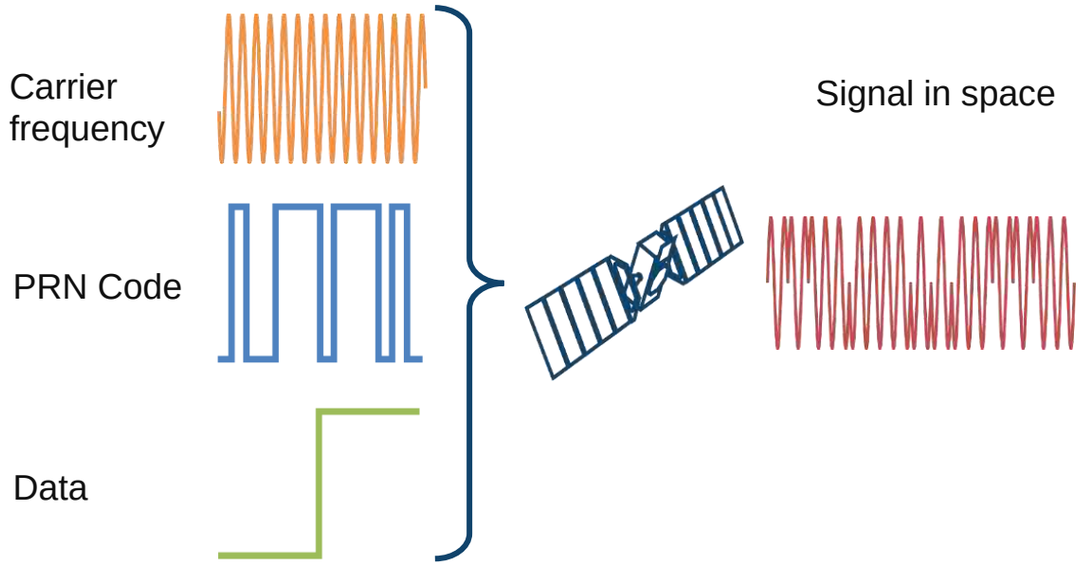


4 global systems and > 40 signals + augmentation systems

Generic GNSS signal structure

The GNSS signal is composed of three components

- Physical layer / carrier frequency
  - Sinusoidal wave → centre frequency (e.g. 1.575 GHz)
- Ranging code layer
  - Distinction of satellites and range estimation using PRN codes
- Data-link layer
  - Navigation message (e.g. satellite position, correction data)



Physical layer and GNSS – carrier wave

- Generation of a fundamental frequency, e.g. for GPS and Galileo, of $f_0 = 10.23$ MHz by atomic frequency standard within the satellite

- Carrier signals in the L-band are generated by integer multiplications of f_0. Examples: using 154, 120 or 115 and denoting the carriers L1, L2 and L5

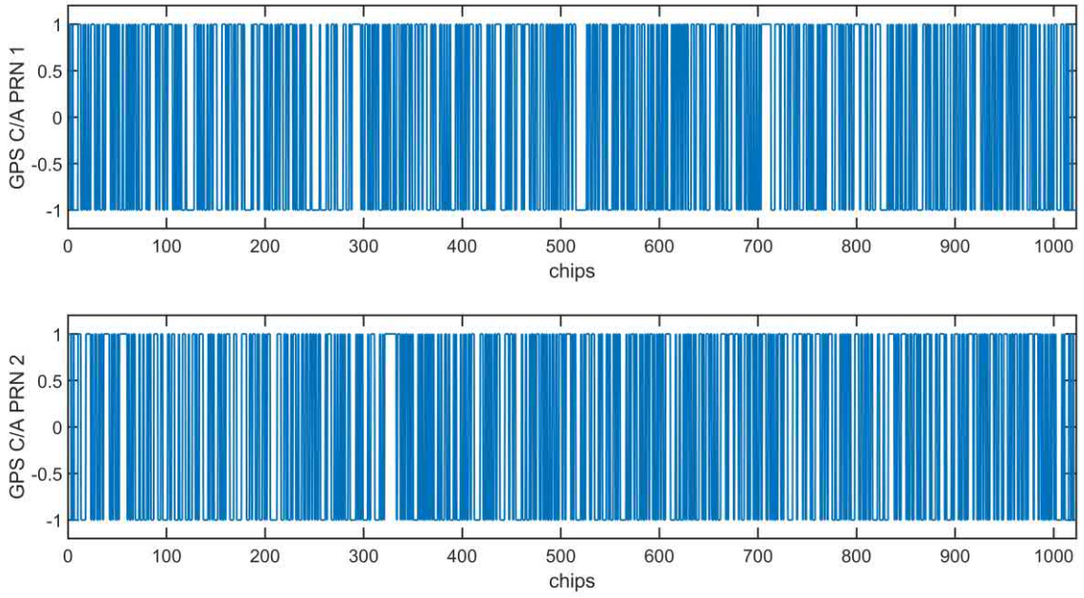
$$\mathrm{L1} = 154\, f_0 = 1575.42\ \mathrm{MHz} \rightarrow \lambda = 19.0\ \mathrm{cm}$$

$$\mathrm{L2} = 120\, f_0 = 1227.60\ \mathrm{MHz} \rightarrow \lambda = 24.4\ \mathrm{cm}$$

$$\mathrm{L5} = 115\, f_0 = 1176.45\ \mathrm{MHz} \rightarrow \lambda = 25.5\ \mathrm{cm}$$

Ranging code layer

- Pseudorandom noise (PRN) code
  - Deterministic sequence of bits
    - The bits of the PRN code are often called “chips” to underscore that these codes do not carry data.
    - Generated either by linear feedback shift register (LFSR) or pre-computed and loaded from memory
  - Special correlation properties
  - Used for
    - Discrimination of satellites (CDMA)
    - Estimation of run-time of the signal (→ code pseudorange)

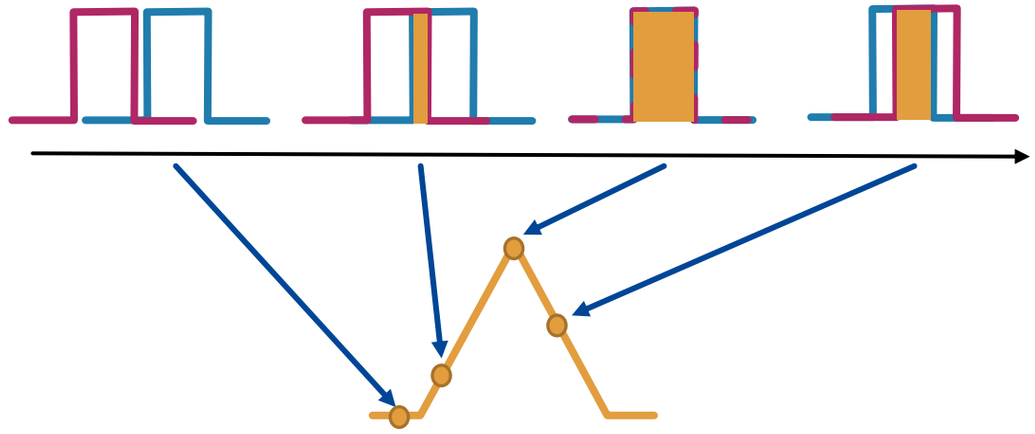


Cross-correlation function

- Cross-correlation function (CCF)
  - describes the degree of correspondence of two signals s1(t) and s2(t)

$$R(\tau) = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} s_1(t) \cdot s_2(t+\tau) dt$$

  - R=1 → s1 = s2
  - R=0 → perfect orthogonality
  - s1(t) = s2(t) → autocorrelation function (ACF)

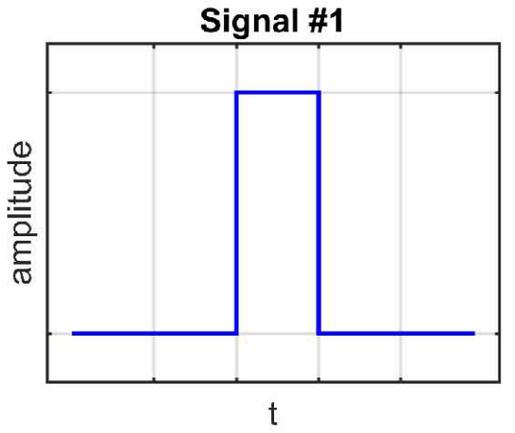


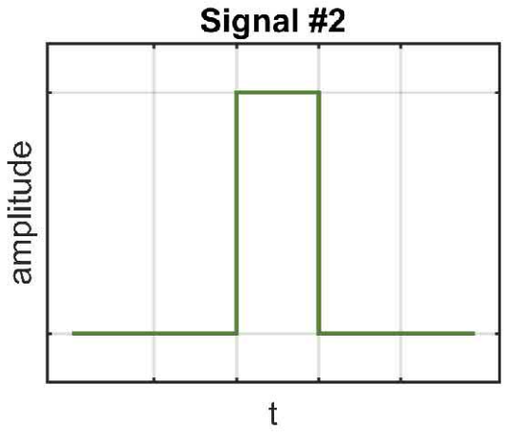
- Properties of GNSS signals
  - maximum correlation at t=0
  - uncorrelated at t ≠ 0
  - uncorrelated with any other PRN sequence

Cross-correlation function – ideal example

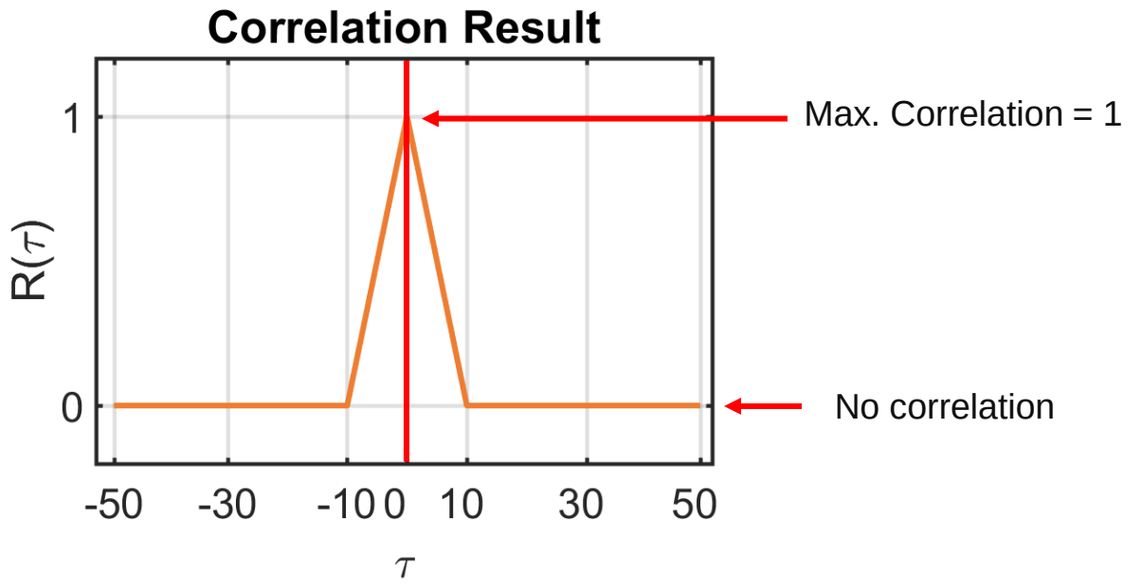
Two signals (Signal #1 and Signal #2)

- Rectangular signal
- $S_1(t) = S_2(t)$ → autocorrelation

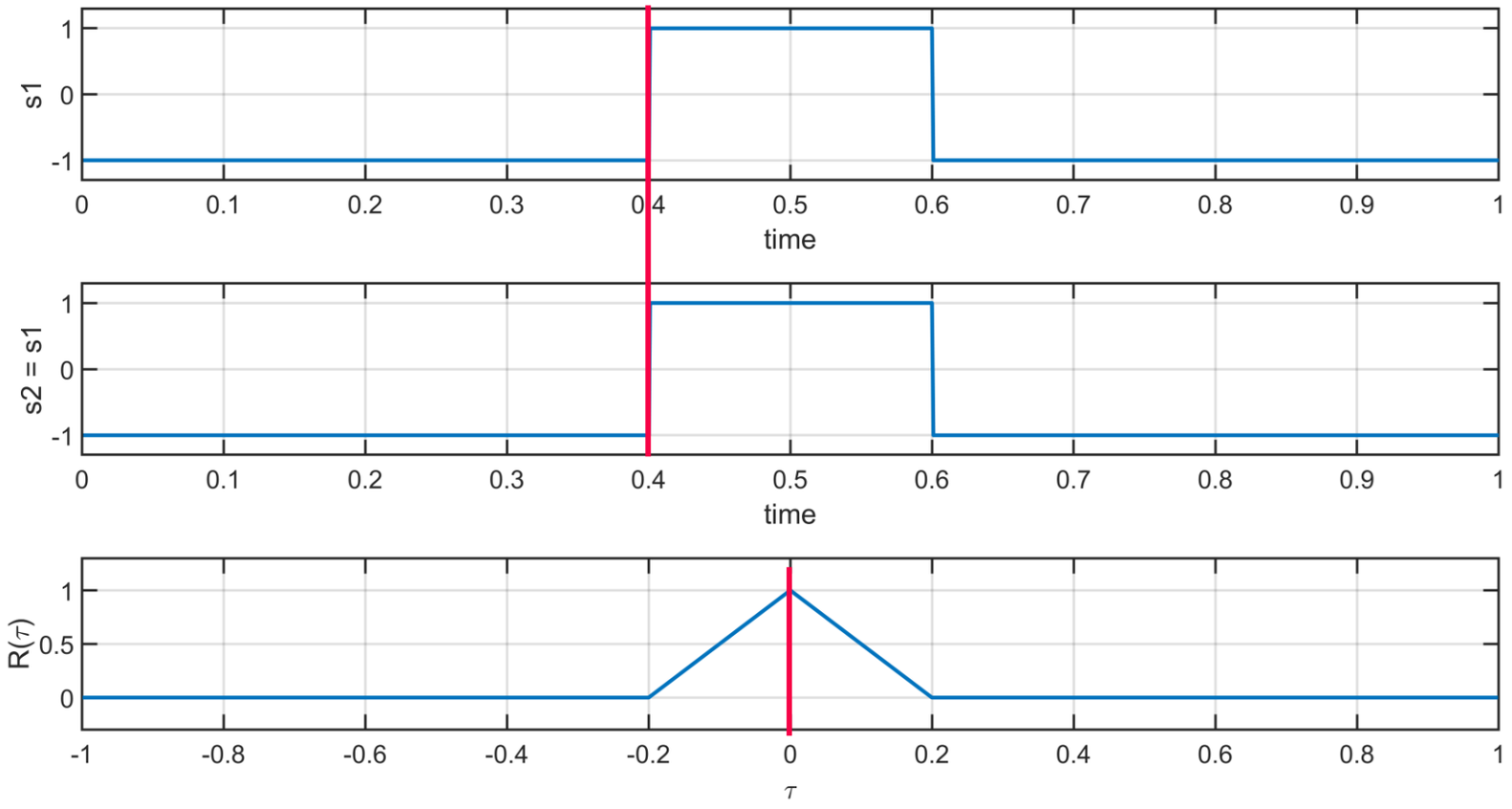




Time shift τ between S_1 and S_2 = 0

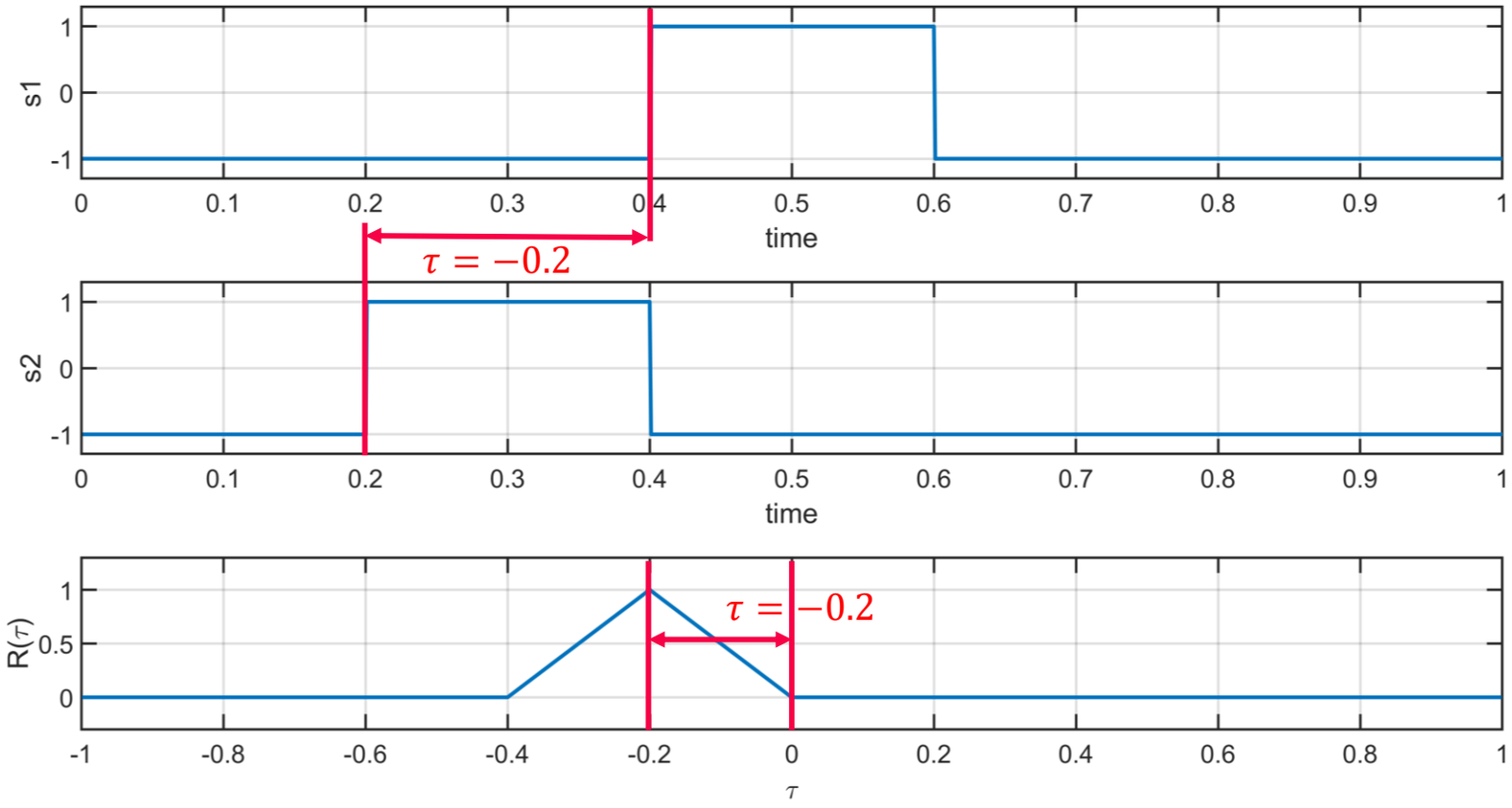


Cross-correlation function – example 1



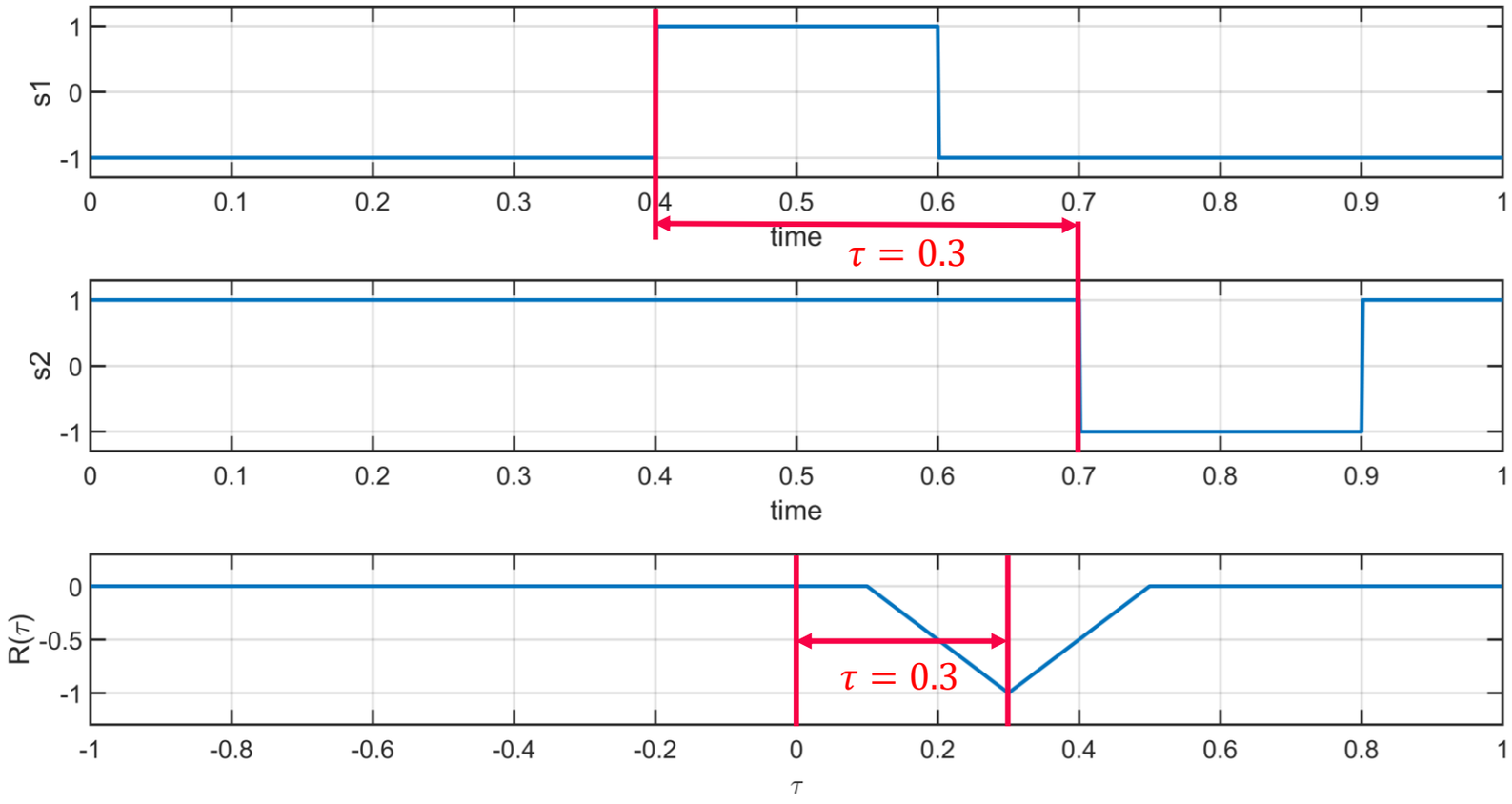
- Auto-correlation
  - s1(t) = s2(t)
- Zero-time lag between s1 and s2 → Maximum at $\tau = 0$

Cross-correlation function – example 2



- Cross-correlation
  - s2(t) = s1(t-τ)
- Time lag $\tau = -0.2$ between s1 and s2
- Location of maximum correlation indicates time shift between signals

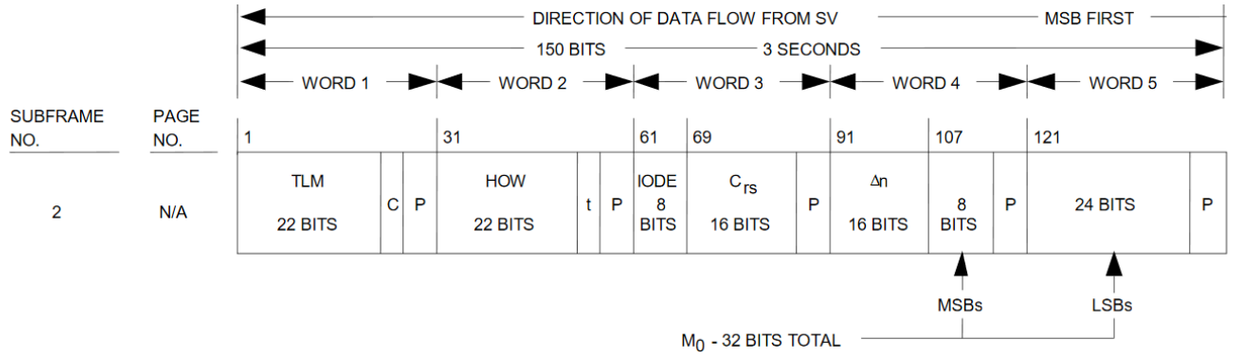
Cross-correlation function – example 3



- Cross-correlation
  - s2(t) = -s1(t-τ)
- Time lag $\tau = 0.3$ between s1 and s2
- $R(\tau) \rightarrow -1$
- Negative correlation peak indicates opposite amplitude

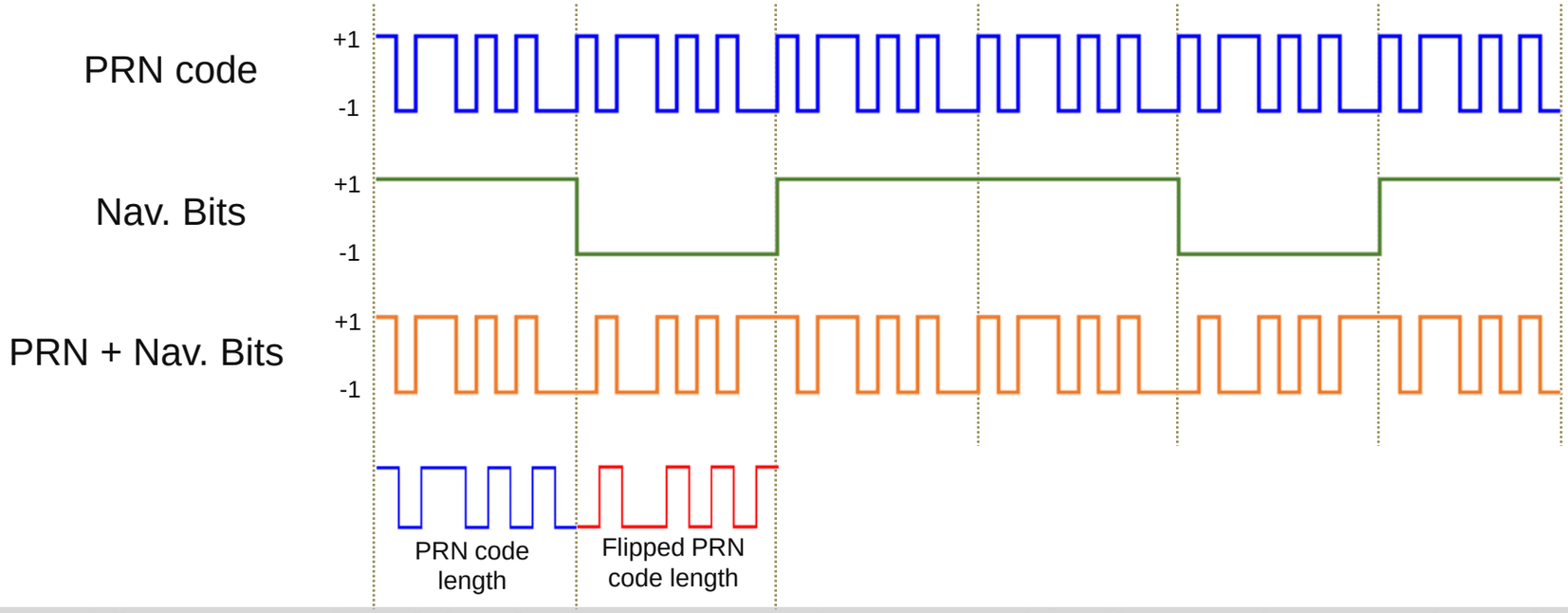
Data-link layer - Navigation data message

- Contains all information necessary to compute, together with the observables, a position, velocity and time solution
  - Time of signal transmission
    (time-of-week and week number)
  - Ephemeris data
    (Keplerian elements and corrections)
  - Satellite clock corrections
  - Ionospheric correction parameters
  - Status and integrity flags
  - Almanac data (orbital data with longer validity)
- Data rates between 50 and 500 bits per seconds
- All parameters are binary coded → coding scheme public available



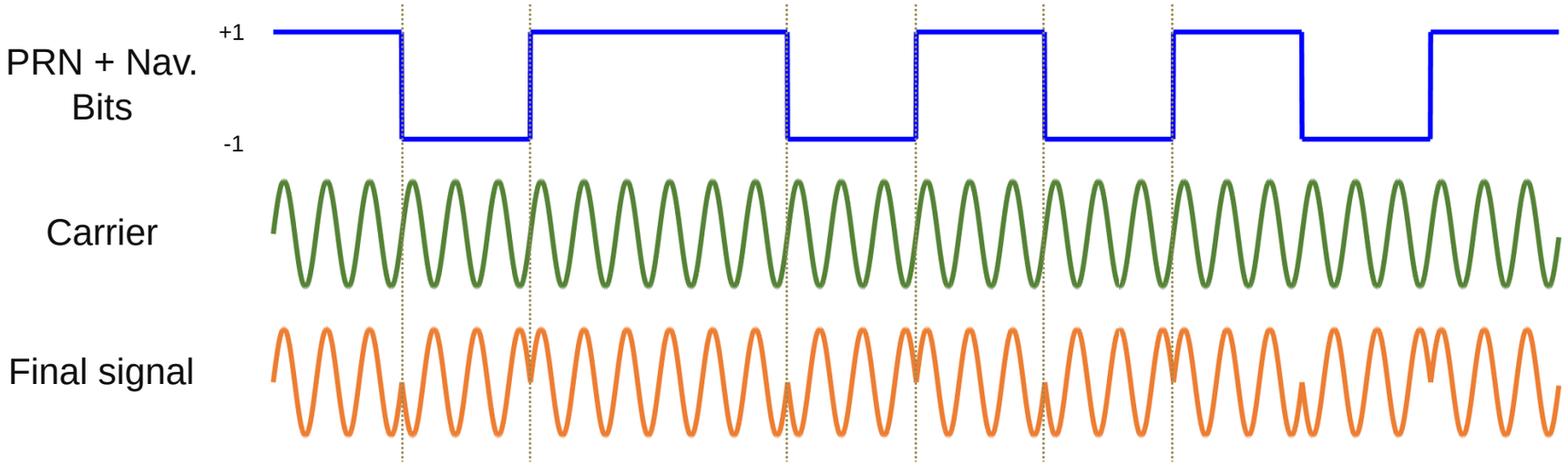
PRN and Navigation Message - Modulation

- Navigation bits are modulo 2 added to the PRN code
  - PRN code flips in case of nav. bit transition flips from 0 to 1 or vice versa
- 1 Navigation bit has the length of one or multiple PRN codes
  (depending on GNSS signal)



Signal Modulation – Binary Phase Shift Keying (BPSK)

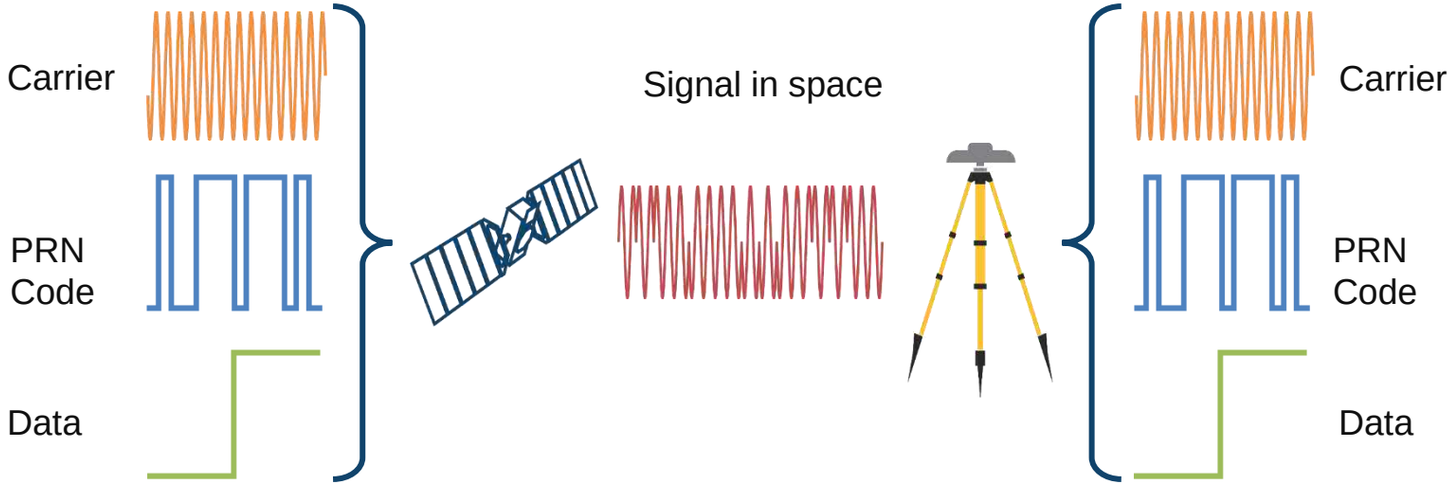
- The code and navigation bits are modulated onto the carrier using biphase modulation
  - Binary Phase Shift Keying (BPSK)
- 180°shift in the carrier phase occurs whenever a change in the code state occurs



GNSS receiver - signal processing

GNSS signal processing

The GNSS signal is composed of three components

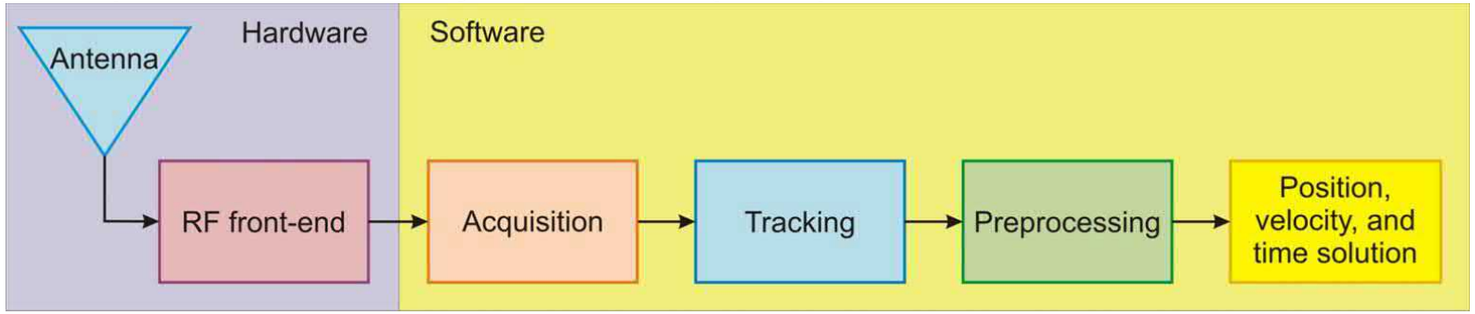


The receiver separates the three components and performs the measurements

- Carrier wave → phase measurement → phase pseudoranges
- PRN-code → run-time → code pseudoranges
- Navigation message → satellite positions

Generic GNSS receiver design

- Purpose of GNSS receiver
  - Receive the signal (antenna)
  - Find visible satellites (acquisition)
  - Track the signal over time (tracking)
    - Split it up into the three components → carrier, PRN code, data
    - Perform runtime measurement (pseudoranges)
  - Decode the navigation data (pre-processing)
  - Compute position, velocity and time (PVT) solution



RF front-end

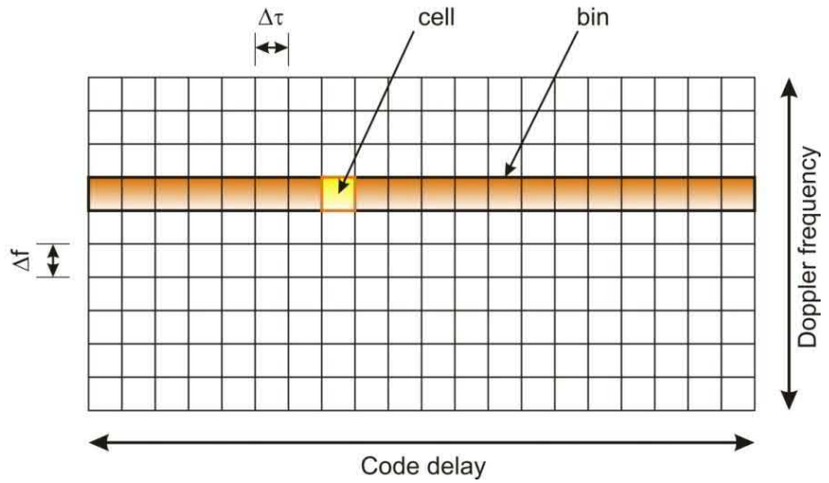
- The goal of the RF front-end is to convert the incoming signals to a lower intermediate frequency, before down-conversion to base-band and A/D conversion
- Analog-Digital Conversion (ADC) involves two operations
  - Sampling
  - Quantization

- ADC implies loss of information → Nyquist-Shannon Sampling Theorem

A continuous-time signal $s(t)$ with the frequencies not higher than f_{max} can be reconstructed exactly from its samples $s[n] = x(nT_s)$, if the sampling rate $f_s = \frac{1}{T_s}$ is greater than twice the bandwidth ($> 2 \cdot f_{max}$).

Signal processing - acquisition

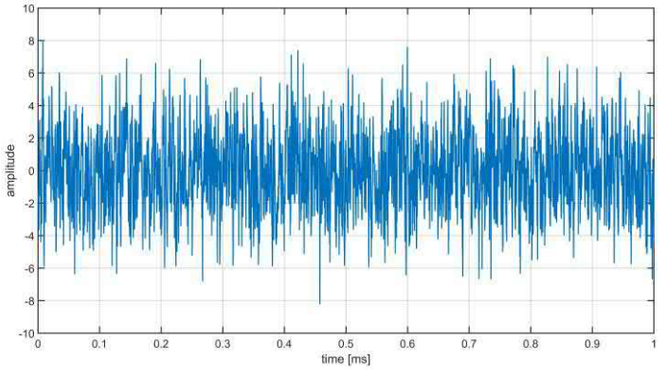
- Acquisition is a search process
  - Decide if satellite signal is present
  - Determine rough estimates of Doppler frequency shift and code phase
- Receiver generates replica signals and correlates them with the incoming signal
  - Since satellites and receiver are moving different code delays and Doppler frequency shifts have to be tested
  - Once a signal has been detected the rough estimates have to be refined and tracked over time
- Doppler search space
  - Relative motion between satellite and receiver
  - Doppler shift: E.g., ±5 kHz up to ±10 kHz

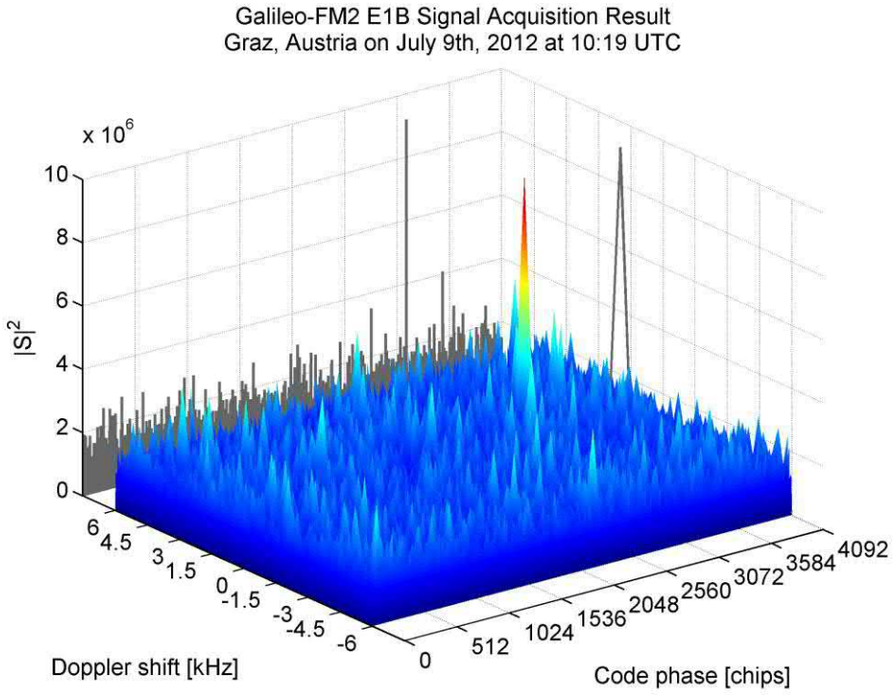


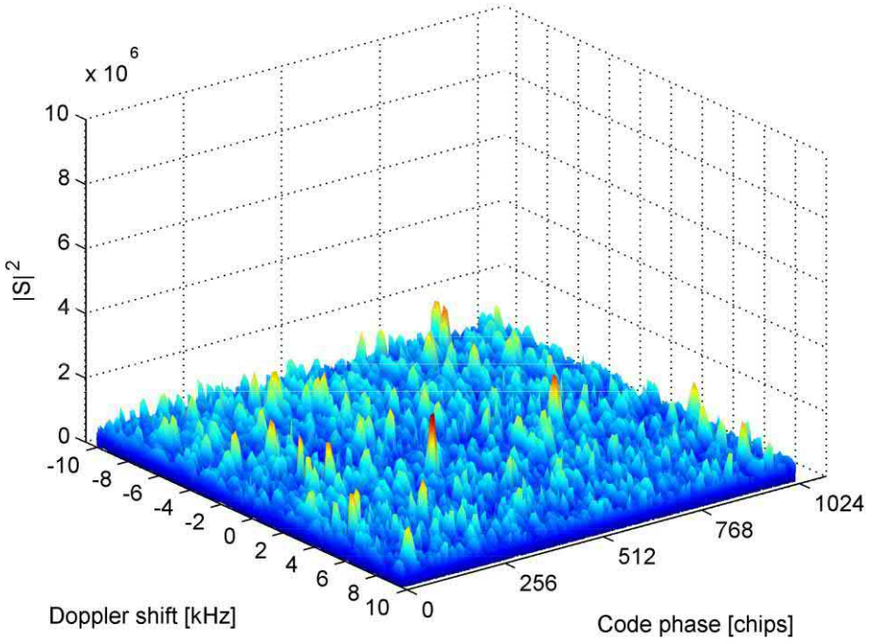
Signal processing - acquisition

- Doppler Search Space
  - Depending on satellite motion and receiver motion
  - Extended search space for space-borne receivers required (!)

Received signal at antenna





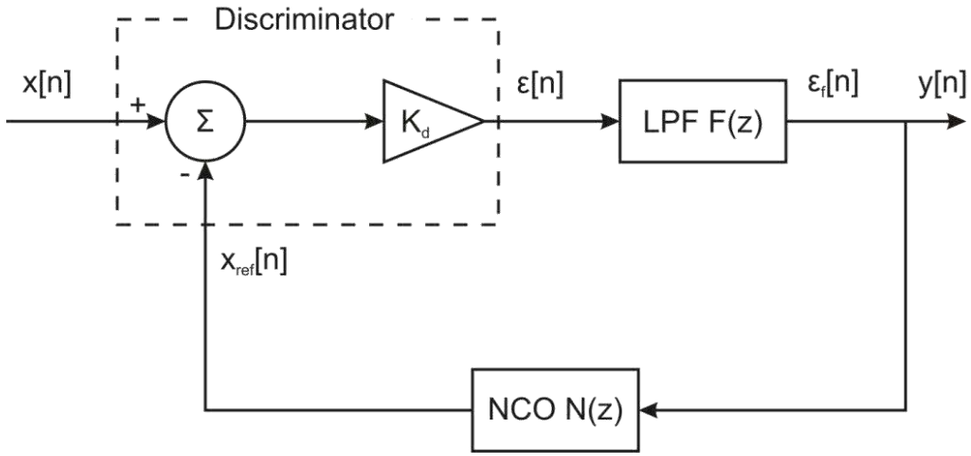


Signal processing - tracking

- Receiver needs to continuously follow the satellite signal
  - Distance between satellite and receiver changes
  - Also the carrier frequency changes due to the relative velocity between satellite and receiver (Doppler)
  - Reception and decoding of navigation message and time of signal transmission
  - Each satellite signal is tracked separately → tracking channels
- Basic principle is signal correlation
  - Receiver generates a replica signal (code and carrier) and performs a correlation
  - Based on the delay estimated within the correlation the next replica signal is adjusted
- This is done within the tracking loops
  - The code ranges are determined in the delay lock loop (DLL)
  - The phase measurement is performed in the phase lock loop (PLL)

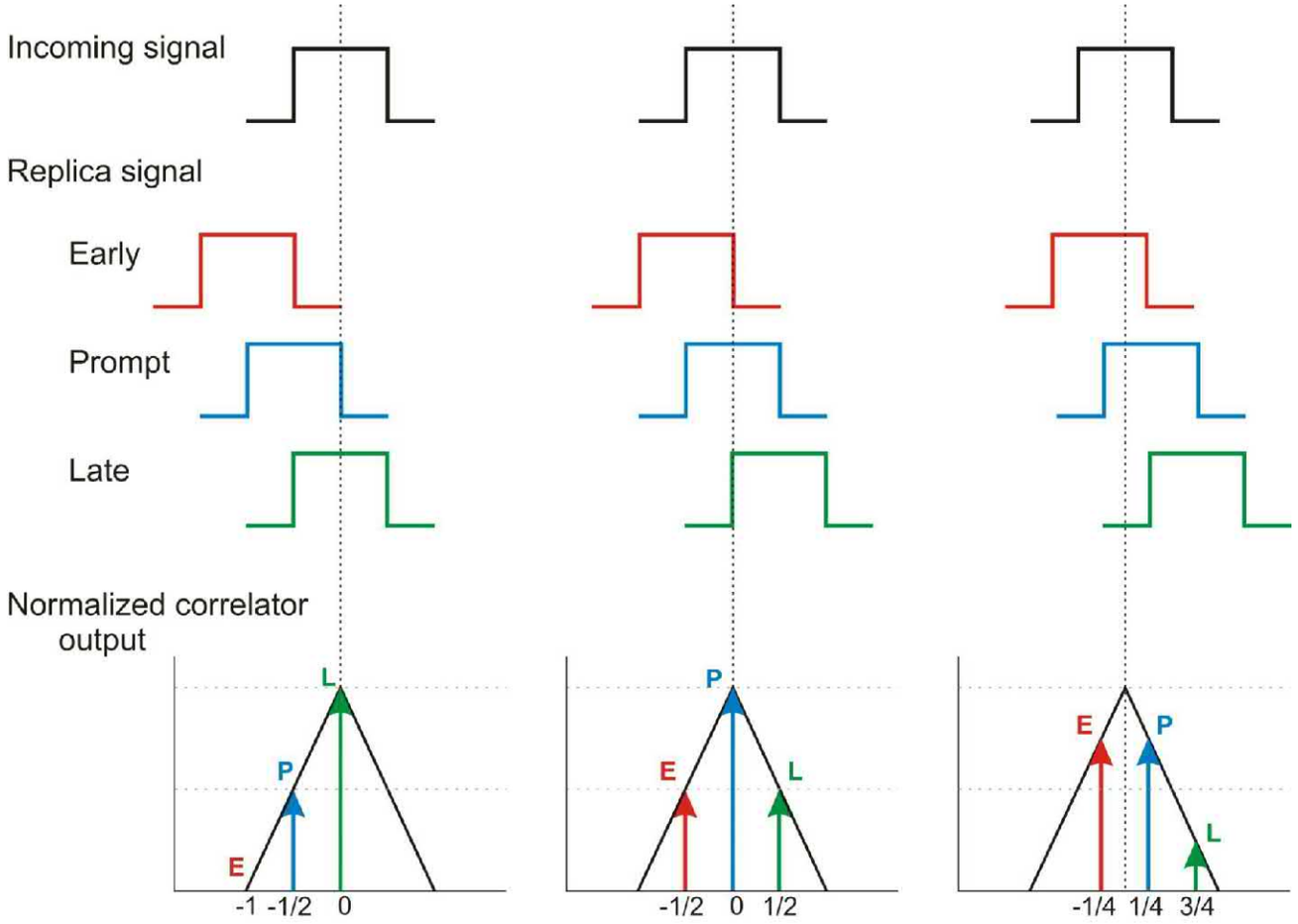
Generic tracking loop

- Generic tracking loop
  - Loop discriminator
  - Integrate & Dump
  - Loop filter
  - Numerical controlled oscillator (receiver clock)
- Carrier tracking
  - Frequency locked loop
  - Phase locked loop
- Code tracking
  - Delay locked loop



Code tracking

- Code tracking uses multiple code replicas (early, prompt, late)
- Delay estimation by using a discriminator function
- Goal to keep the prompt at zero delay and early and late correlation values at the same level

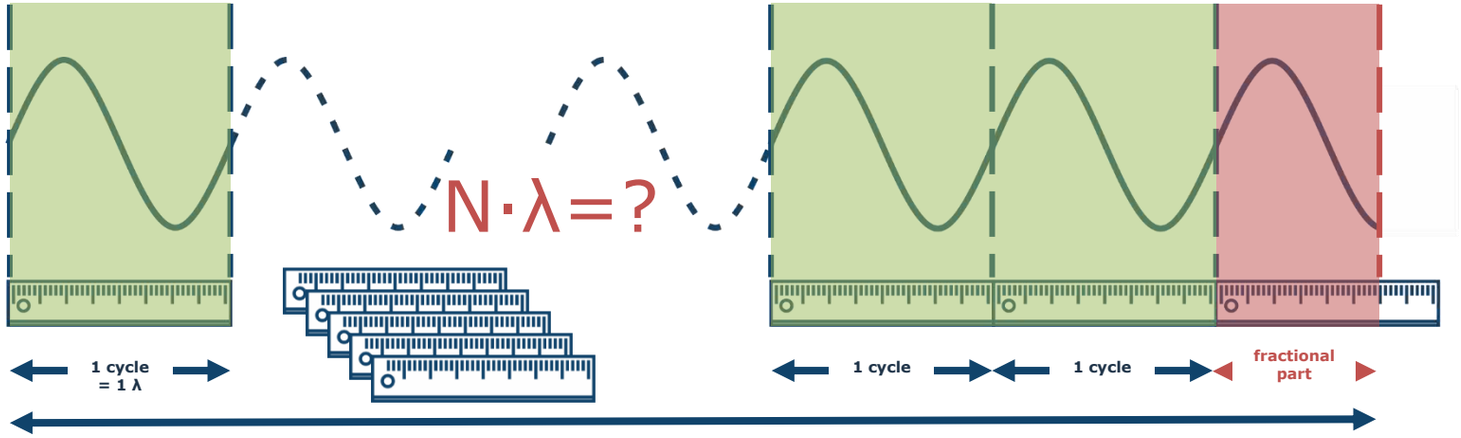


Carrier tracking

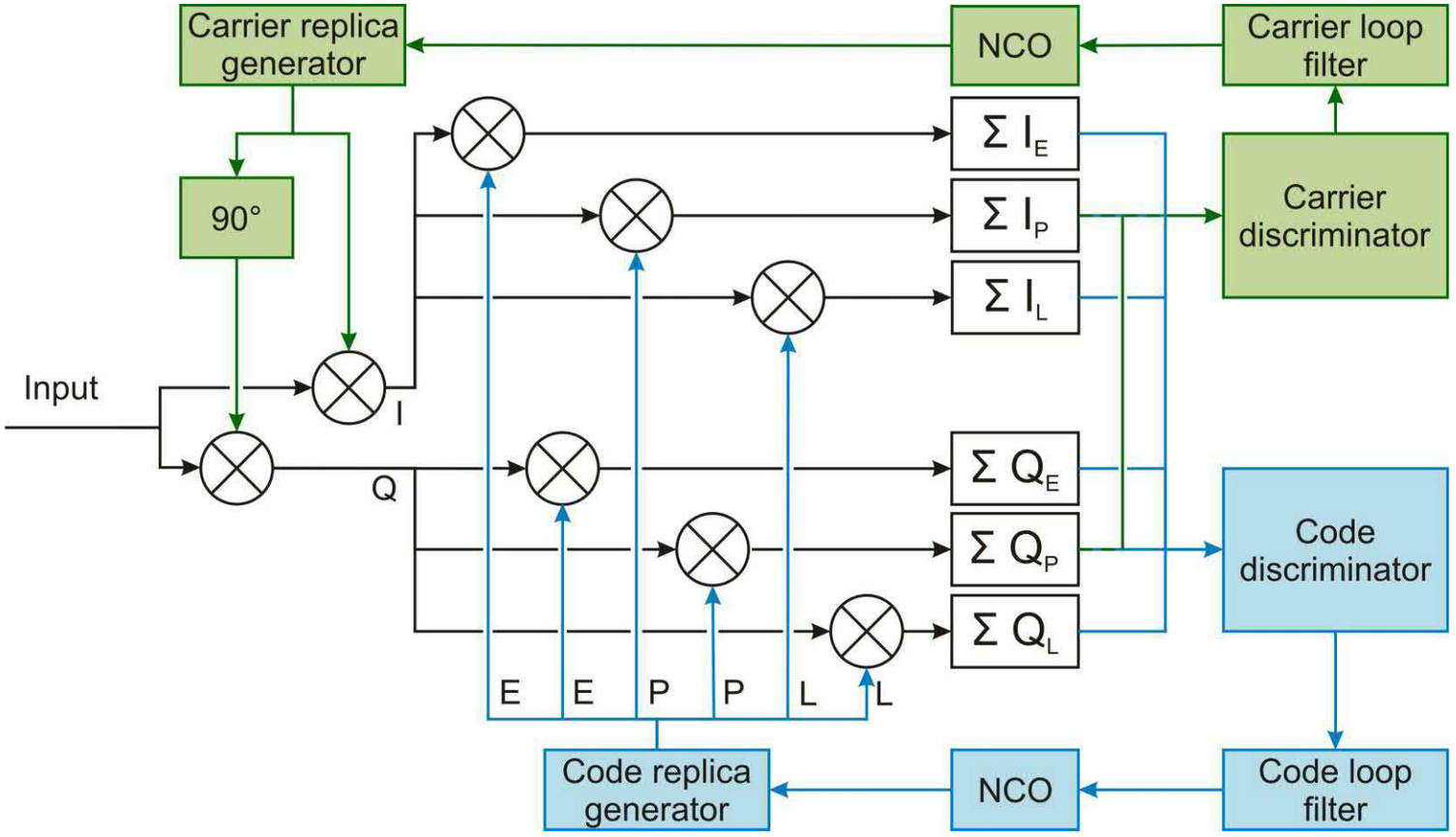
- The phase lock loop looks very similar to the delay lock loop
- Instead of code replicas sine and cosine carrier waves are used
- The continuous phase observable is obtained by counting the elapsed cycles and by measuring the fractional part of the phase of the correlated locally generated signal
- Cycle slips occur within this measurement when the elapsed cycles are not correctly counted, and loss of lock when the two signals are no longer continuously correlated

Carrier phase measurement

- Distance (range) between satellite and receiver can be expressed in terms of the number of wavelengths of the signal carrier
  - Wavelength of, e.g. GPS L1 C/A, carrier λ = 19 cm = 1 cycle
- Only the fractional part of the last cycle can be measured by the receiver
  - Resolution of up to 1/100 of a wavelength
- The integer number of the cycles is not known → ambiguity

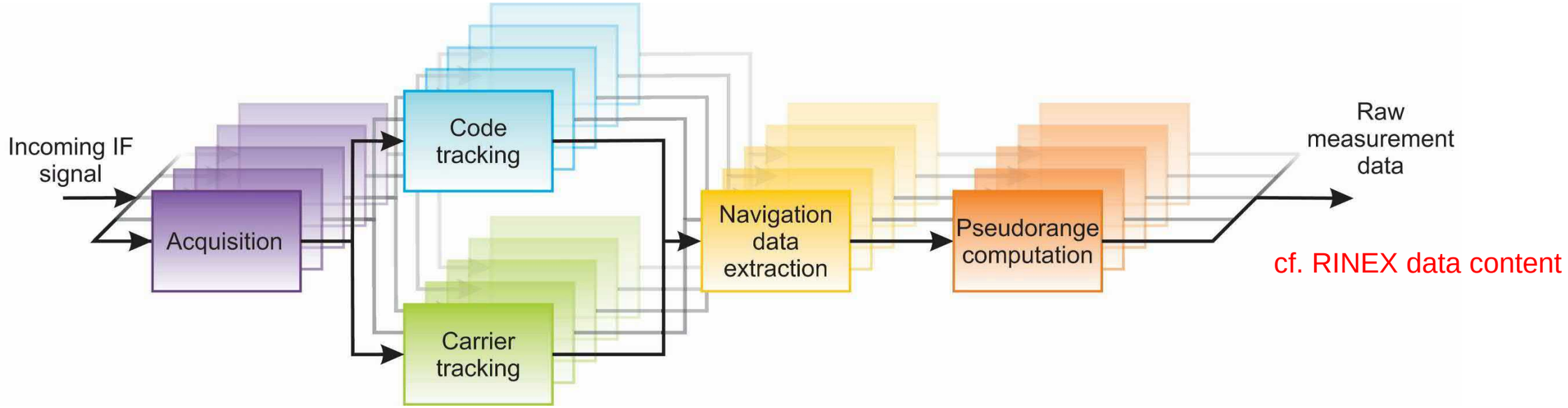


Tracking module / channel



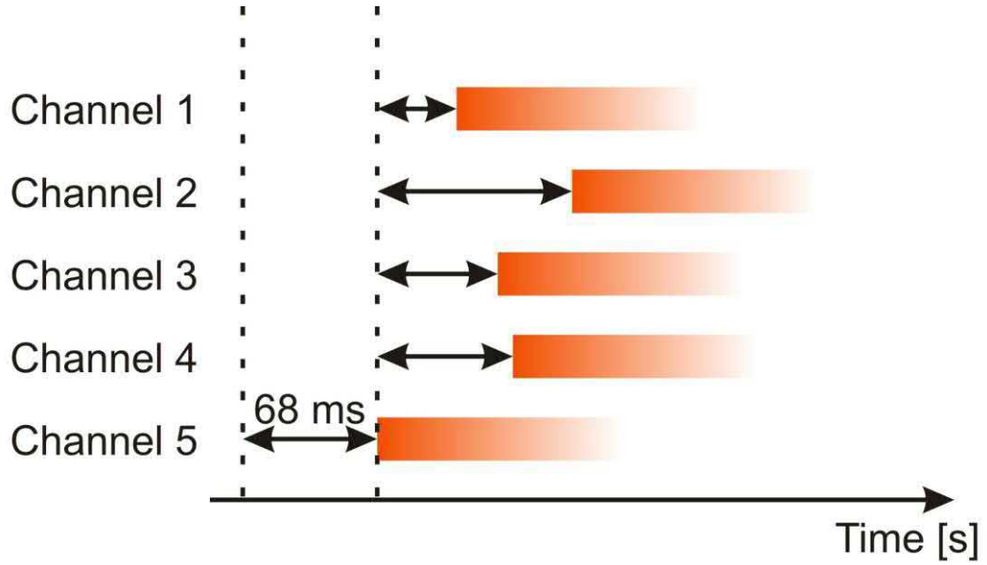
Receiver channels

- Tracking is executed for every signal/satellite individually → receiver channels
- Output of tracking: Measurements (i.e. pseudoranges, phase measurements, Doppler) & navigation message content

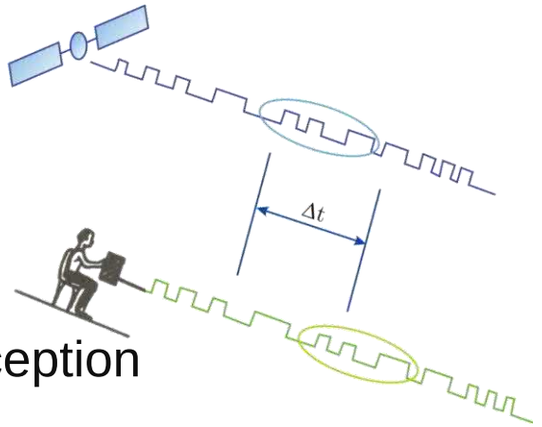


Pseudorange computation

- Pseudorange computation is based on time of signal emission and time of signal reception
- First bit of a navigation message subframe (first bit of preamble) is used for timing (time of signal reception and related to time of signal transmission)



Code ranging



- Determination of the travelled distance based on
  - cross-correlation between satellite signal and replica
  - Retrieval of time of transmission within the navigation message
- Runtime estimated based on time of signal emission and time of signal reception

$$t_r(rec) - t^s(sat) = [t_r + \delta_r] - [t^s + \delta^s] = \Delta t_r^s + \Delta\delta_r^s$$

- Multiplication by speed of light c leads to Pseudorange R

$$R_r^s = c \cdot \Delta t_r^s + c \cdot \Delta\delta_r^s = \rho_r^s + c \cdot \Delta\delta_r^s$$

R_r^s … pseudorange between satellite and receiver
ρ_r^s … geometric distance between satellite and receiver
$\Delta\delta_r^s$ … combined satellite-receiver clock error

Carrier phase measurement

$$\Phi_r^s(t) = \frac{1}{\lambda}\rho_r^s(t) + \frac{c}{\lambda}\Delta\delta_r^s(t) + N_r^s$$

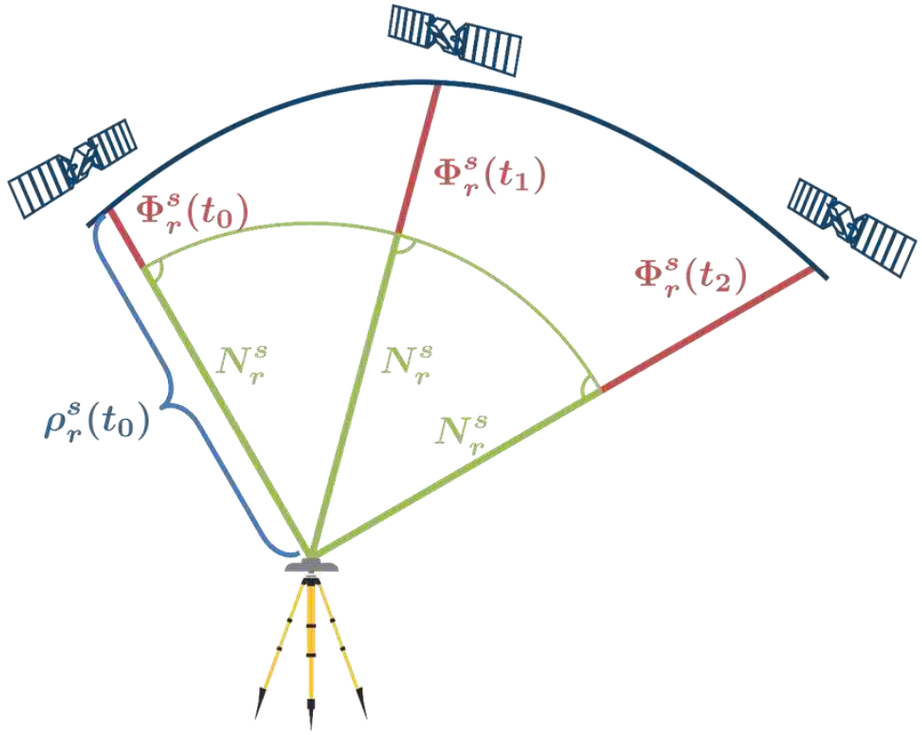
$\Phi_r^s(t)$ … carrier phase measurement [cycles]

$\rho_r^s(t)$ … geometric distance (range) [m]

$\Delta\delta_r^s(t)$ … combined clock error [s]

$$\Delta\delta_r^s(t) = (\delta_r(t) - \delta^s(t))$$

N_r^s … integer ambiguity [cycles]

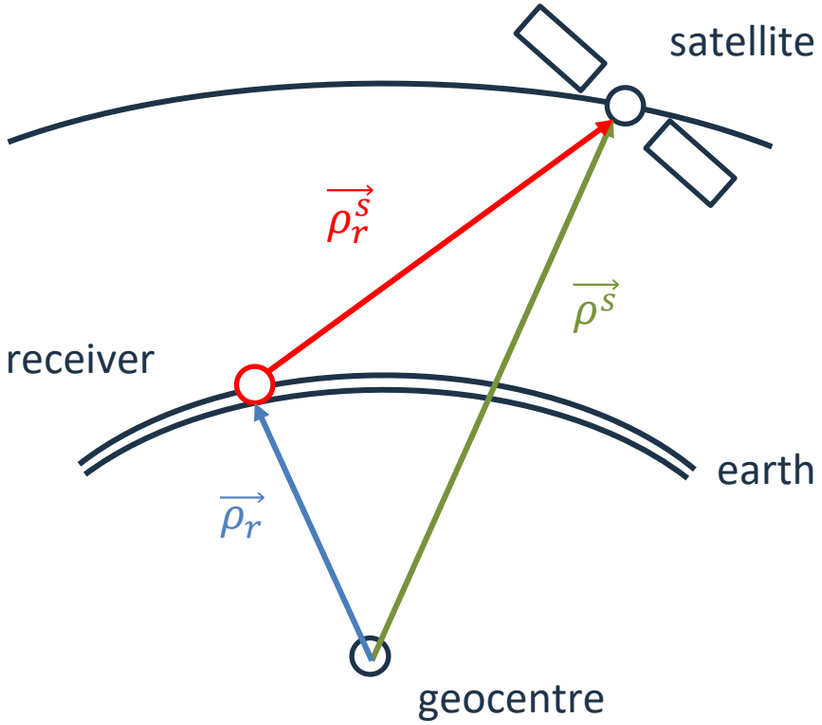


- Note that this is an ideal, error free model and all remaining range errors and corrections have been neglected
- Phase measurements are far more precise

Be aware of the units and the conversion factors. $f = \frac{c}{\lambda}$

Basic principle of Satellite Geodesy

- Satellite geodesy
  - Orbit determination
    (receiver position known)
  - Positioning
    (satellite position known)



- Geometric observations
  (e.g. ranges) are measured

$$\rho_r^s = \left\| \overrightarrow{\rho_r^s} \right\| = \sqrt{(X^s - X_r)^2 + (Y^s - Y_r)^2 + (Z^s - Z_r)^2}$$

Principle of position determination

Principle is based on runtime time measurements (distances) between the satellites and the receiver

- Known satellite position (transmitted by satellite)
- Intersection of spheres

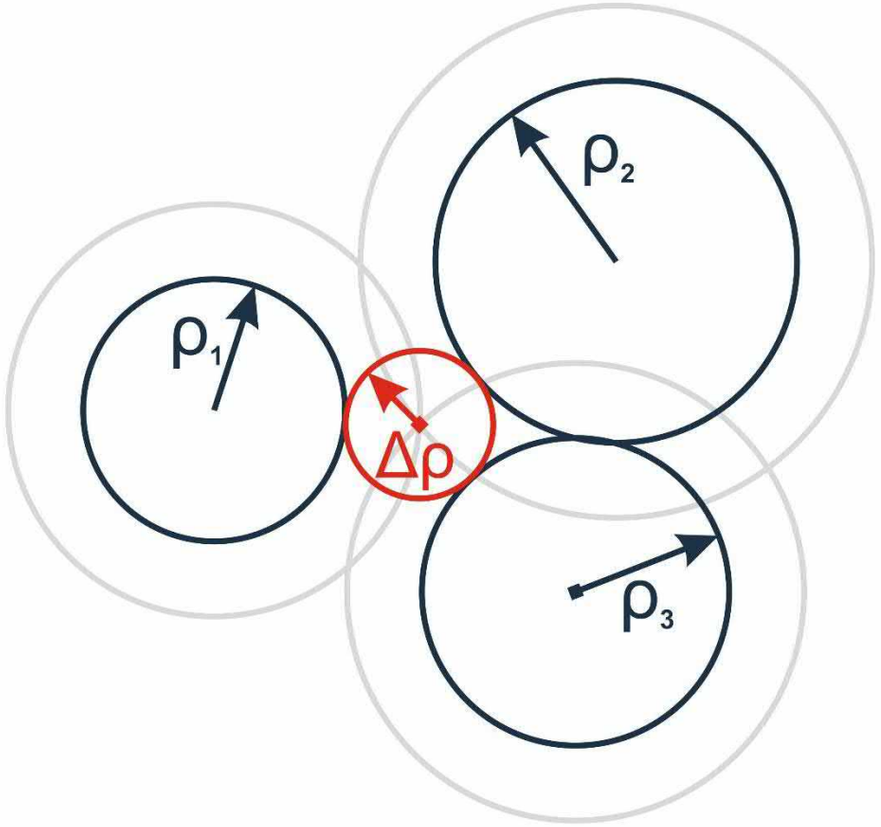
Unsynchronized satellite and receiver clocks

- No intersection
- Additional uncertainty
- Pseudorange measurements

Additional measurement (at least 4 satellites) necessary

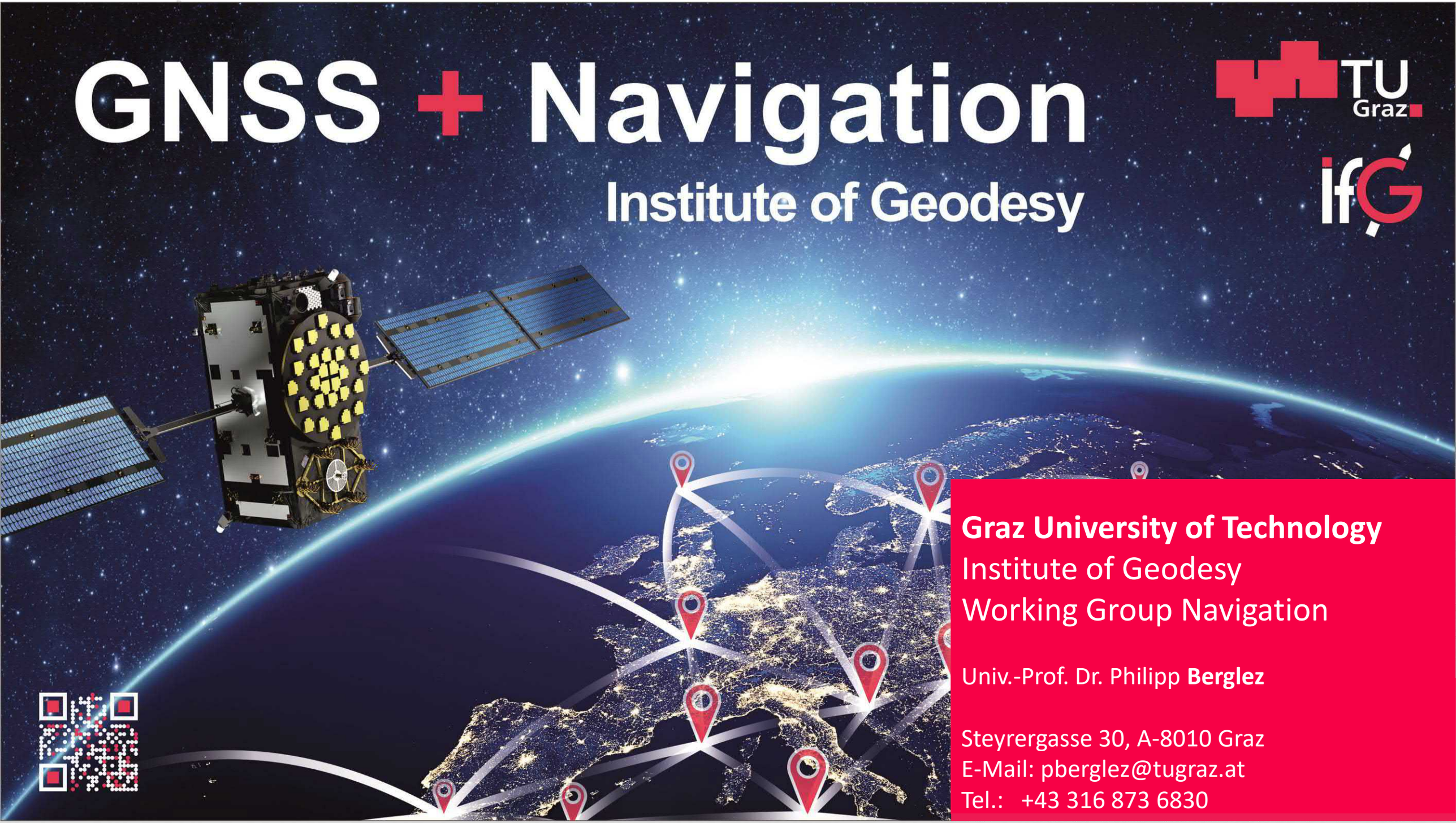
- Coordinates (X,Y,Z) + clock error

$$R_r^s(t) = \rho_r^s(t) + c \cdot \Delta\delta_r^s(t)$$



GNSS + Navigation

Institute of Geodesy



Graz University of Technology
Institute of Geodesy
Working Group Navigation

Univ.-Prof. Dr. Philipp **Berglez**

Steyrergasse 30, A-8010 Graz
E-Mail: pberglez@tugraz.at
Tel.: +43 316 873 6830