Technische Universität Berlin
Flugführung
und Luftverkehr

GNSS Under Attack

How GNSS Works – A Technical Primer for All

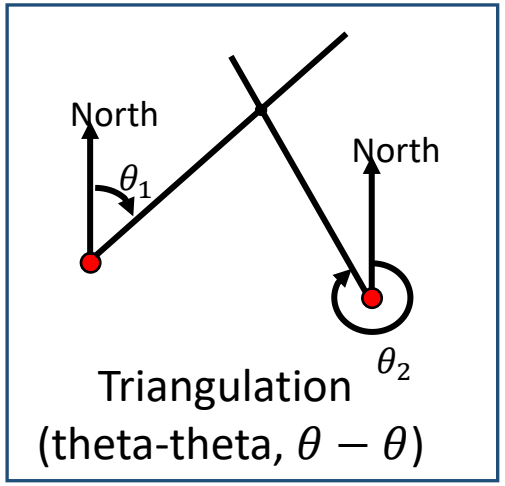
Lecture – 9:15-9:45

Prof. Dr. ir. Maarten Uijt de Haag

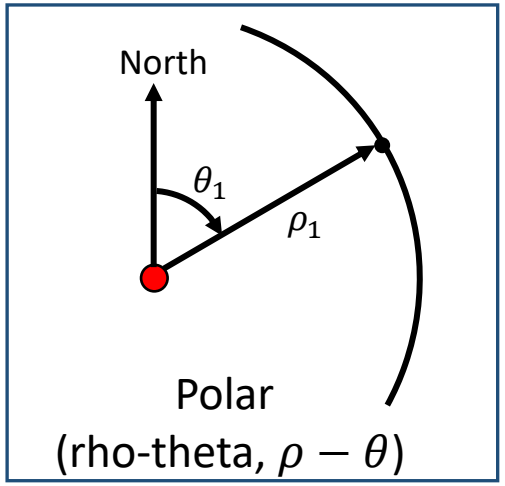
Institute of Aeronautics and Astronautics
Chair of Flight Guidance and Air Transport

Technische Universität Berlin
Flugführung und Luftverkehr

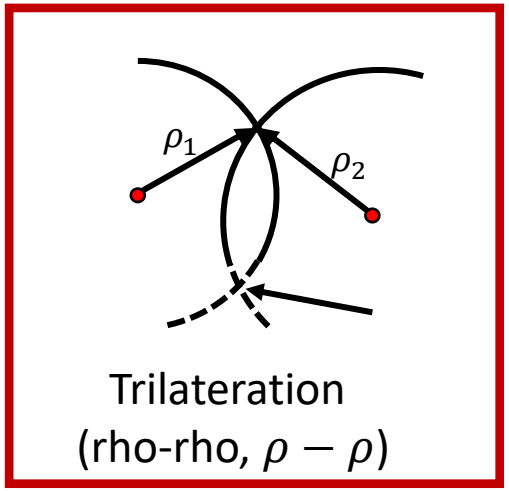
Position Determination



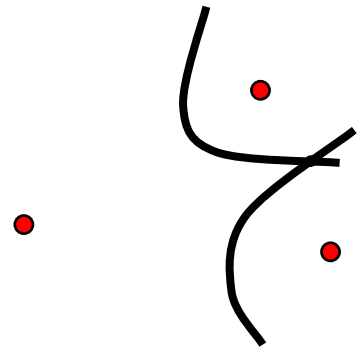
Triangulation
(theta-theta, $\theta - \theta$)



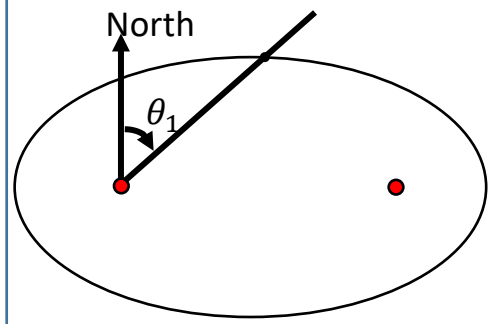
Polar
(rho-theta, $\rho - \theta$)



Trilateration
(rho-rho, $\rho - \rho$)



Hyperbolic/elliptical



Combination

So, how about GNSS?

*Position Determination is also known as position fixing

Technische Universität Berlin
Flugführung und Luftverkehr

Two-Dimensional $\rho - \rho$ Positioning

Foghorn Example

Source: wikipedia

A foghorn or fog signal is a device that uses sound to warn vehicles of navigational hazards such as rocky coastlines, or boats of the presence of other vessels, in foggy conditions

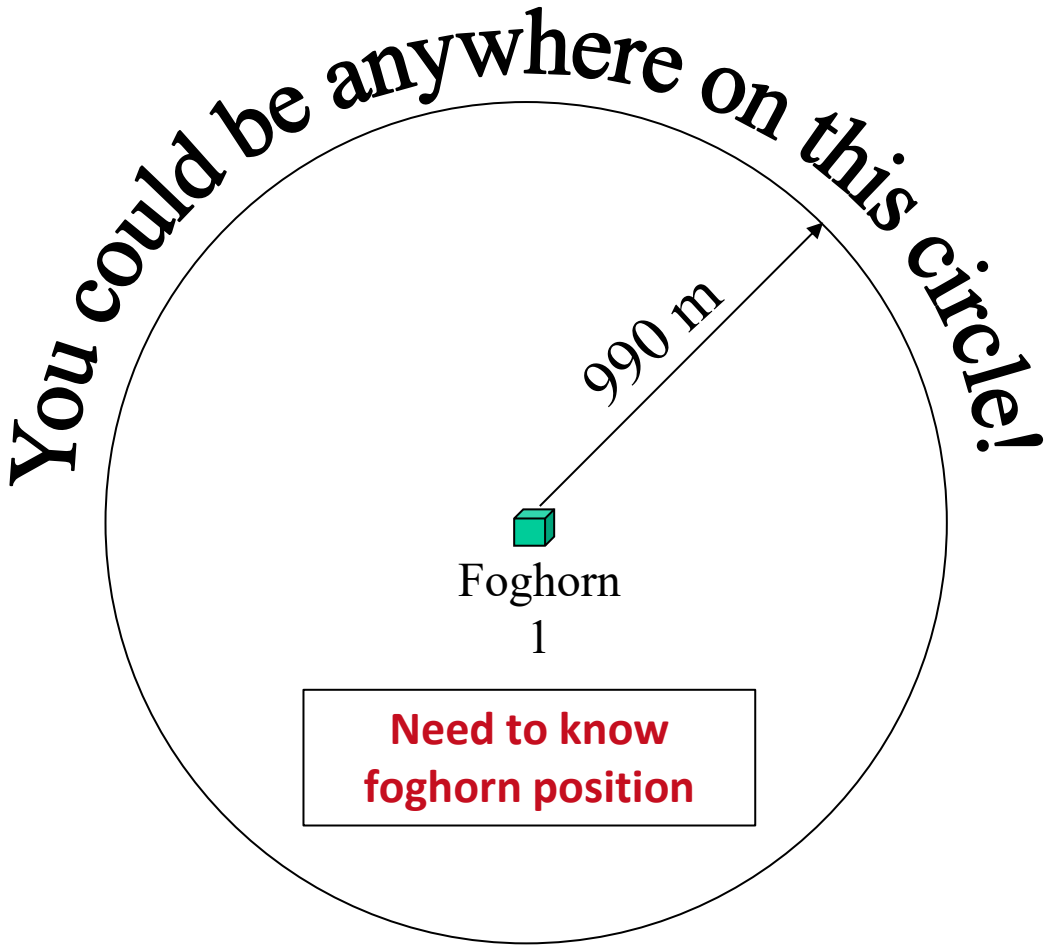
Technische Universität Berlin
Flugführung und Luftverkehr

Two-Dimensional $\rho - \rho$ Positioning

- Foghorn sends signal at **12:00:00**
  - **Time-of-Transmission** (**TOT**)
- Receiver receives message at **12:00:03**
  - **Time-of-Arrival** (**TOA**) or **Time-of-Reception** (**TOR**)
- Speed of sound:
  - v_{sound} = 330m/s
- Range between you and the foghorn (#1) is:

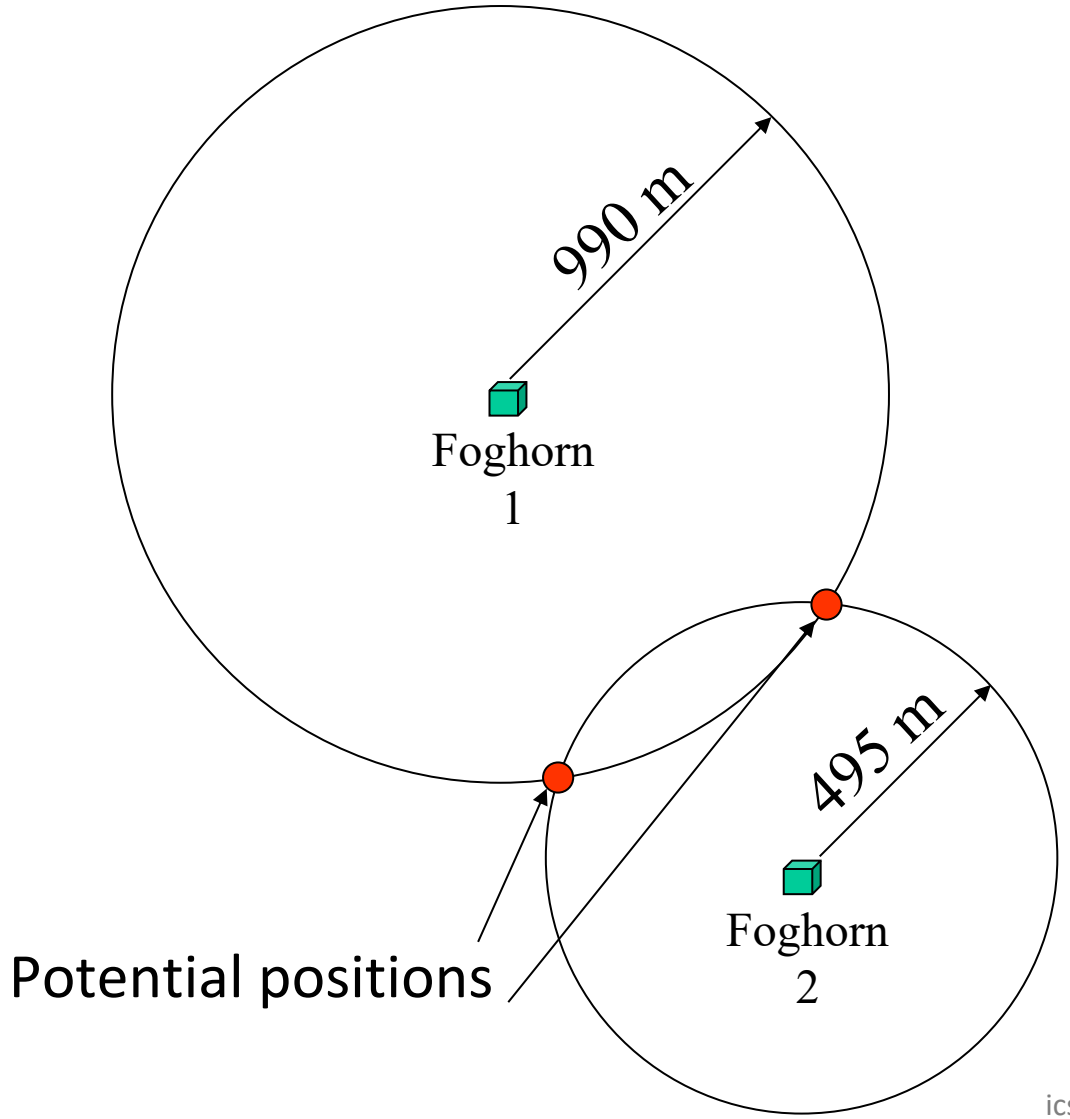
$$R = v_{sound}(\mathrm{TOR} - \mathrm{TOT}) = v_{sound}\Delta t = 990m$$

- Unable to determine exact position in this case



Two-Dimensional $\rho - \rho$ Positioning

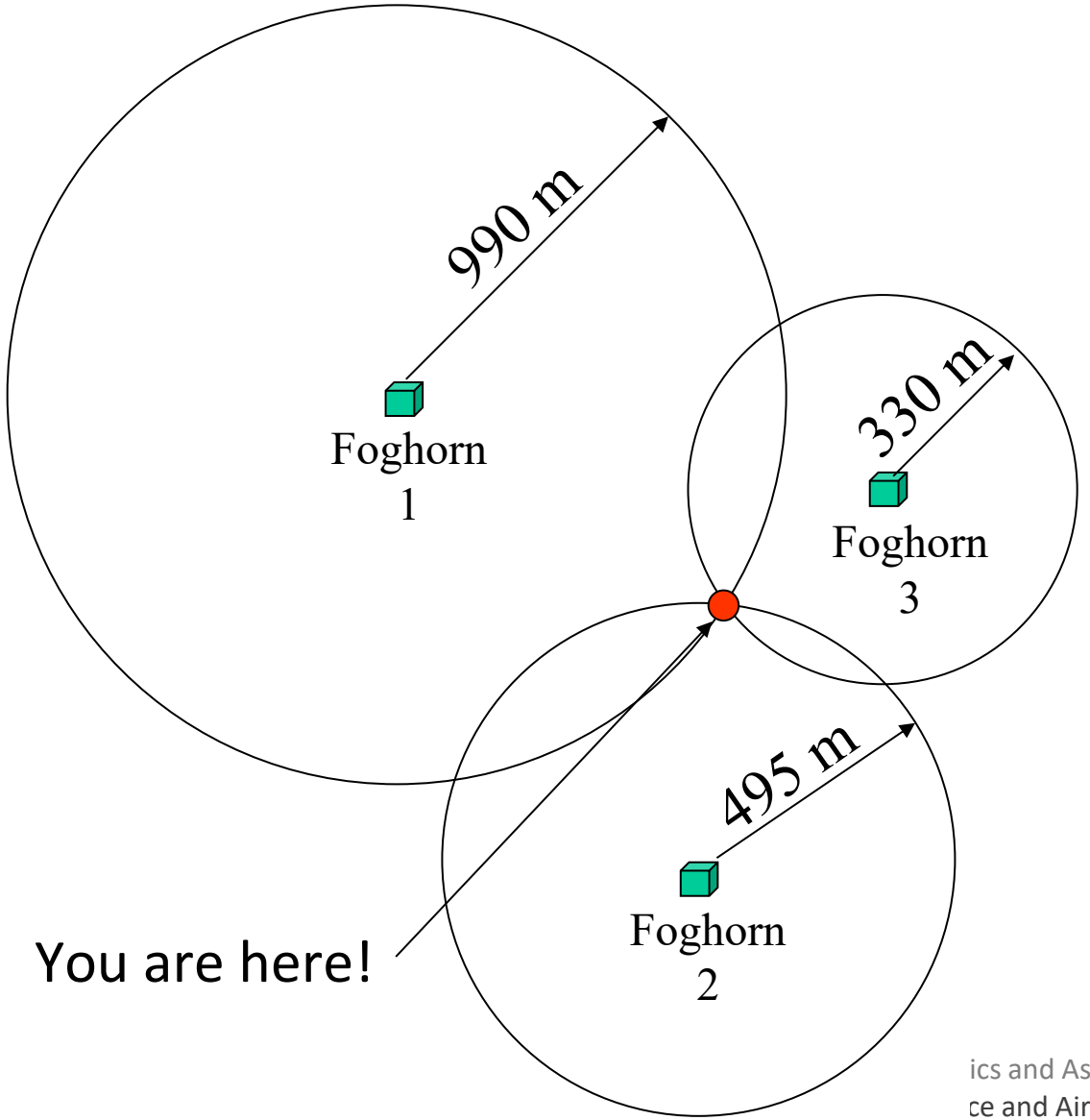
- Now, you take a measurement from foghorn #2 at TOA = **12:00:01.5** (for a range of **495 m**)
- Yields two potential solutions
  - How would you determine the correct solution?



Two-Dimensional $\rho - \rho$ Positioning

- You get a third measurement from foghorn #3 at TOA = **12:00:01**
- Range = **330 m**
  - Now there's a unique solution

Important:
Clocks of all Foghorns must be synchronized and their locations known



Technische Universität Berlin
Flugführung und Luftverkehr

Receiver Clock Errors

- The foghorn example assumed that the foghorn "**receiver**" had a perfectly synchronized clock, so the measurements were perfect
- What happens if there is an **unknown receiver clock error** between the receiver clock and the Foghorn clocks?
- Effect on range measurement
  - Without clock error

$$R = v_{sound}(TOA - TOT) = v_{sound}\Delta t$$

  - With clock error δt

$$PR = v_{sound}(TOA + \delta t\ - TOT) = v_{sound}(\Delta t + \delta t)$$

Range with error (referred to as: **pseudo-range**)

Technische Universität Berlin
Flugführung und Luftverkehr

Receiver Clock Errors – 1D Example

- Now, we will look at the foghorn example, except in only one dimension
  - The foghorn(s) and receiver are constrained to be along a line
  - We want to determine the position of the receiver on that line

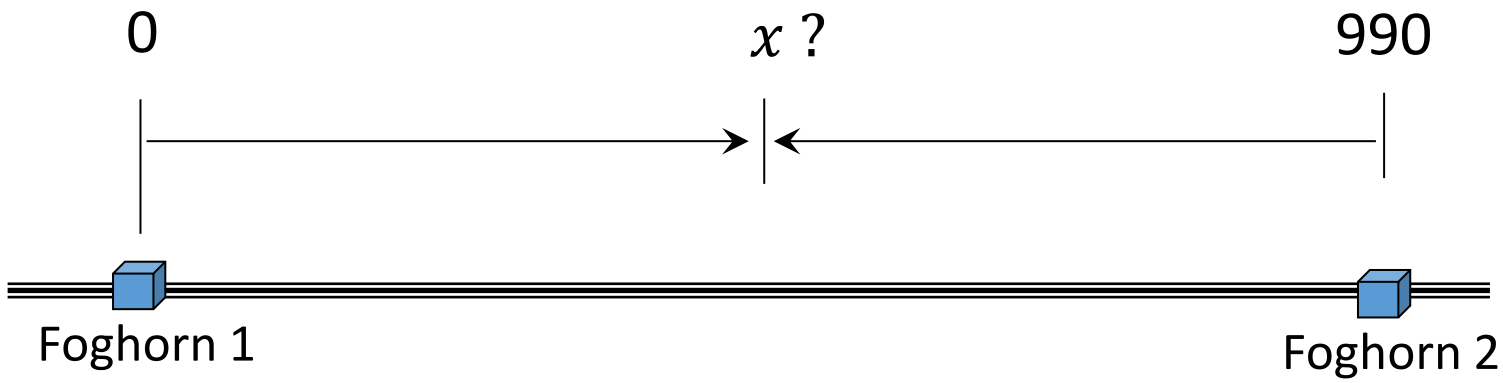
Foghorn 1

- If the receiver measured a signal at **12:00:10**, where is it on the line?
- Now, assume an unknown clock bias δt in the clock used by the foghorn receiver
- Your foghorn receiver measures a foghorn blast at **12:00:10**
- What can you say about where you are?

Technische Universität Berlin
Flugführung und Luftverkehr

Receiver Clock Errors – 1D Example

- Clearly, more information is needed
- Assume that there is a second foghorn located 990 m away from the first

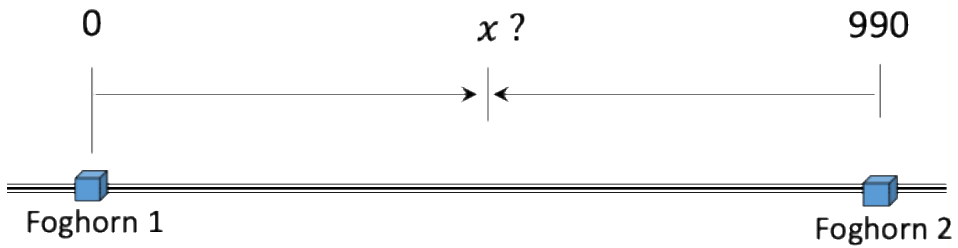


- You receive a signal from the second foghorn at **12:00:09**
- What can you tell about where you are at this point?

Receiver Clock Errors – 1D Example

- Here are the **pseudorange measurements** we have:

$$PR_1 = v_{sound} \times 10 = 330 \times 10 = 3300$$
$$PR_2 = v_{sound} \times 9 = 330 \times 9 = 2970$$



- From the **pseudorange** equation:

$$PR_1 = v_{sound}(\Delta t_1 + \delta t) = R_1 + v_{sound}\delta t = x + v_{sound}\delta t = 3300$$
$$PR_2 = v_{sound}(\Delta t_2 + \delta t) = R_2 + v_{sound}\delta t = 990 - x + v_{sound}\delta t = 2970$$

- Rearranging terms we get

$$x + v_{sound}\delta t = 3300$$
$$x - v_{sound}\delta t = -1980$$

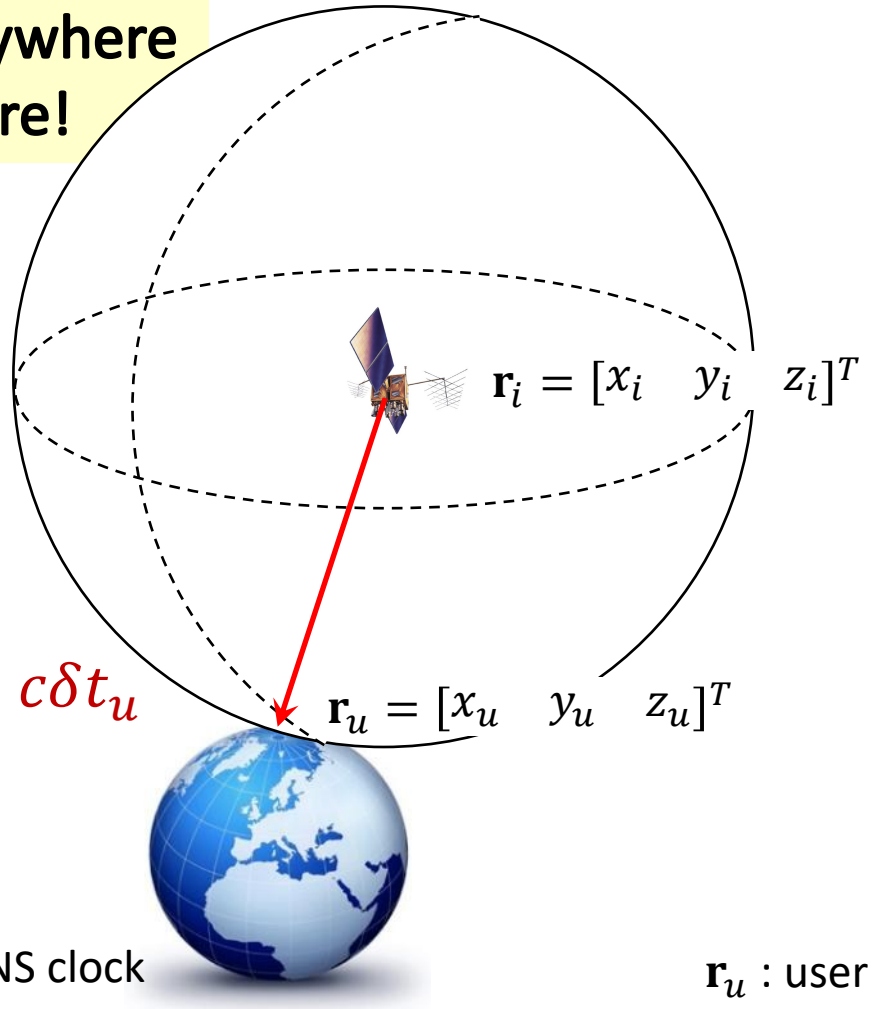
- We can then solve for the two unknowns

$$\delta t = 8\ seconds$$
$$x = 660m$$

Technische Universität Berlin
Flugführung und Luftverkehr

GNSS – from 2D to 3D

You could be anywhere on this sphere!



Foghorn → GNSS Satellite

Circles → Spheres

Speed of sound → Speed of light

Pseudorange:

$$PR_i = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2} + c\delta t_u$$

$$= \|\mathbf{r}_u - \mathbf{r}_i\| + c\delta t_u$$

Euclidean distance between user and satellite position

Difference between the user clock and the GNNS clock

$\mathbf{r}_u$: user position

$\mathbf{r}_i$: satellite 'i' position

Technische Universität Berlin
Flugführung und Luftverkehr

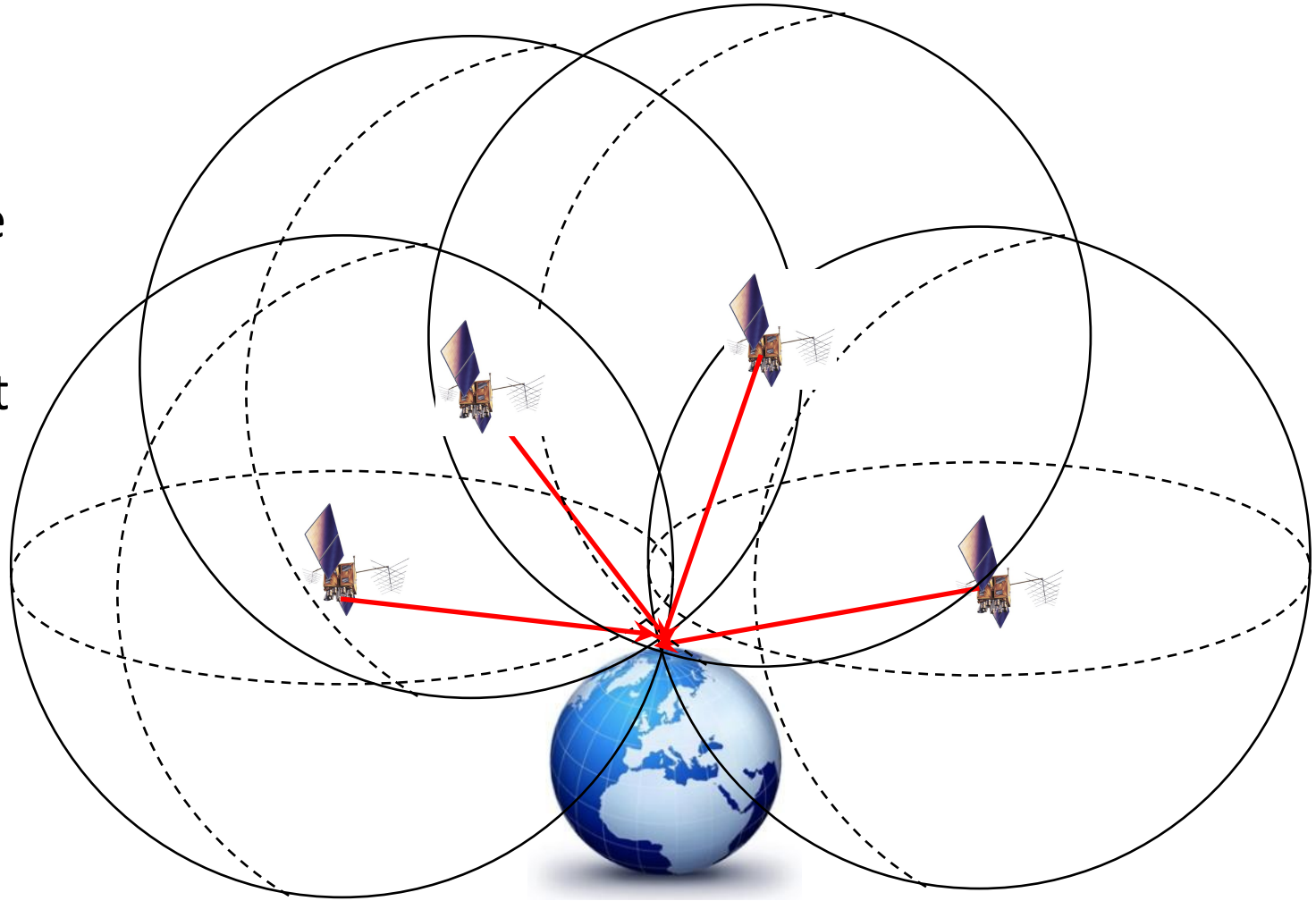
GNSS – from 2D to 3D

Foghorn → GNSS Satellite

Circles → Spheres

Speed of sound → Speed of light

User is on the intersection of at least 4 spheres



Technische Universität Berlin
Flugführung und Luftverkehr

Receiver Clock Errors – Extend to 3D

- In the **single-dimensional** case
  - We needed two measurements to solve for the two unknowns, x and δt.
  - The quantities x and $(990 - x)$ were the "distances" between the position of the receiver and the two foghorns.
- In **three-dimensional** case
  - We need four measurements to solve for the four unknowns, x, y, z and δt.
  - The distances between receiver and satellite are not linear equations (as was case in single-dimensional case).
  - The >four equations to be solved simultaneously, for **pseudorange** measurements $PR_1 \ldots PR_N$ and **transmitter positions** $(x_1, y_1, z_1) \ldots (x_N, y_N, z_N)$

$$PR_j = \sqrt{(x_u - x_j)^2 + (y_u - y_j)^2 + (z_u - z_j)^2} + c\delta t_u$$

Technische Universität Berlin
Flugführung und Luftverkehr

Approaches to solve these equations

- Closed form solutions
  - Complicated
  - May not give as much insight
- Iterative techniques based on linearization
  - Often using least-squares estimation
  - Arguably the simplest approach
- Kalman filtering
  - Similar to least-squares approach, except with additional ability to handle measurements over a period of time

Ordinary Least Squares Solution

$$PR_j = \sqrt{(x_u - x_j)^2 + (y_u - y_j)^2 + (z_u - z_j)^2} + c\delta t_u$$

$$\Delta PR_j = \frac{\partial PR_j}{\partial x_u}\Delta x_u + \frac{\partial PR_j}{\partial y_u}\Delta y_u + \frac{\partial PR_j}{\partial z_u}\Delta z_u + c\delta t_u$$

$$\Delta PR_j = \frac{x_u - x_j}{R_j}\Delta x_u + \frac{y_u - y_j}{R_j}\Delta y_u + \frac{z_u - z_j}{R_j}\Delta z_u + c\delta t_u$$

$$\Delta\mathbf{PR} = \begin{bmatrix} \frac{x_u - x_1}{R_1} & \frac{y_u - y_1}{R_1} & \frac{z_u - z_1}{R_1} & 1 \\ \frac{x_u - x_2}{R_2} & \frac{y_u - y_2}{R_2} & \frac{z_u - z_2}{R_2} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \frac{x_u - x_N}{R_N} & \frac{y_u - y_N}{R_N} & \frac{z_u - z_N}{R_N} & 1 \end{bmatrix} \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ c\delta t_u \end{bmatrix} = \mathbf{H}\Delta\mathbf{x}$$

$$\Delta\hat{\mathbf{x}} = \left(\mathbf{H}^{\mathrm{T}}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathrm{T}}\Delta\mathbf{PR}$$

$$\hat{\mathbf{x}}_{k+1} = \hat{\mathbf{x}}_k + \Delta\hat{\mathbf{x}}$$

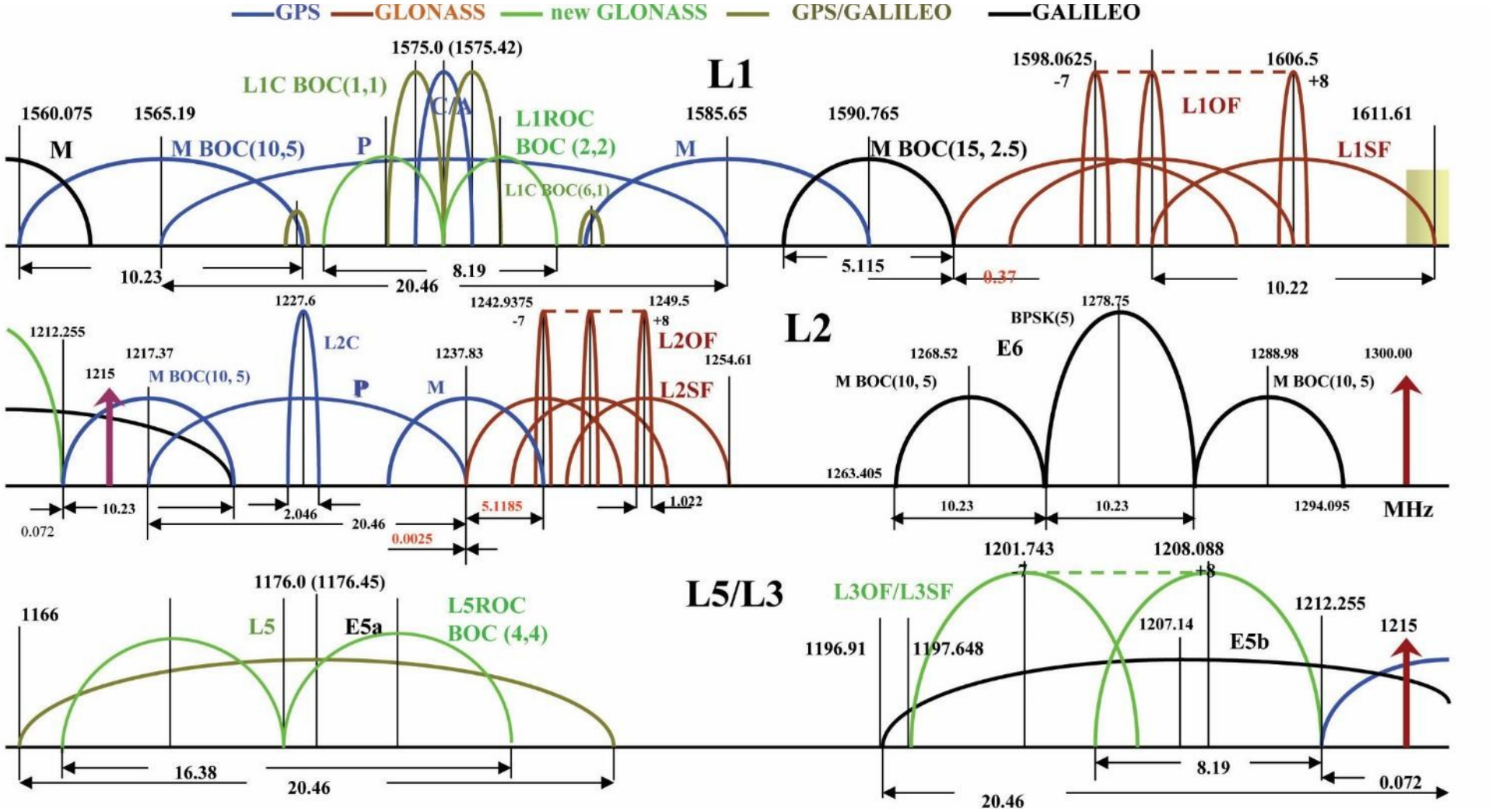
Various Systems

System	Source	Coding	Frequencies	Status (1 February 2026)
Global Positioning System (GPS)	United States	CDMA	L1 (1575.42MHz) L2 (1227.60MHz) L5 (1176.45MHz)	Operational (28)
GLONASS	Russia	FDMA/CDMA	FDMA (1602 MHz) FDMA (1246 MHz) CDMA (1600.995MHz) CDMA (1248.06MHz) CDMA (1202.25MHz)	Operational (24 - nominal)
Galileo	European Union	CDMA	E1 (1575.420MHz) E6 (1278.750MHz) E5 (1191.795MHz) E5a (1176.450MHz) E5b (1207.140MHz)	Operational (26)
BeiDou	China	CDMA	B1 (1561.098MHz) B1-2 (1589.742MHz) B2 (1207.140MHz) B3 (1268.52MHz)	Operational (30~35)

Status info:
GPS: https://www.navcen.uscg.gov/gps-constellation
Galileo: https://www.gsc-europa.eu/system-service-status/constellation-information
GLONASS: https://glonass-iac.ru/en/GLONASS/

Technische Universität Berlin
Flugführung und Luftverkehr

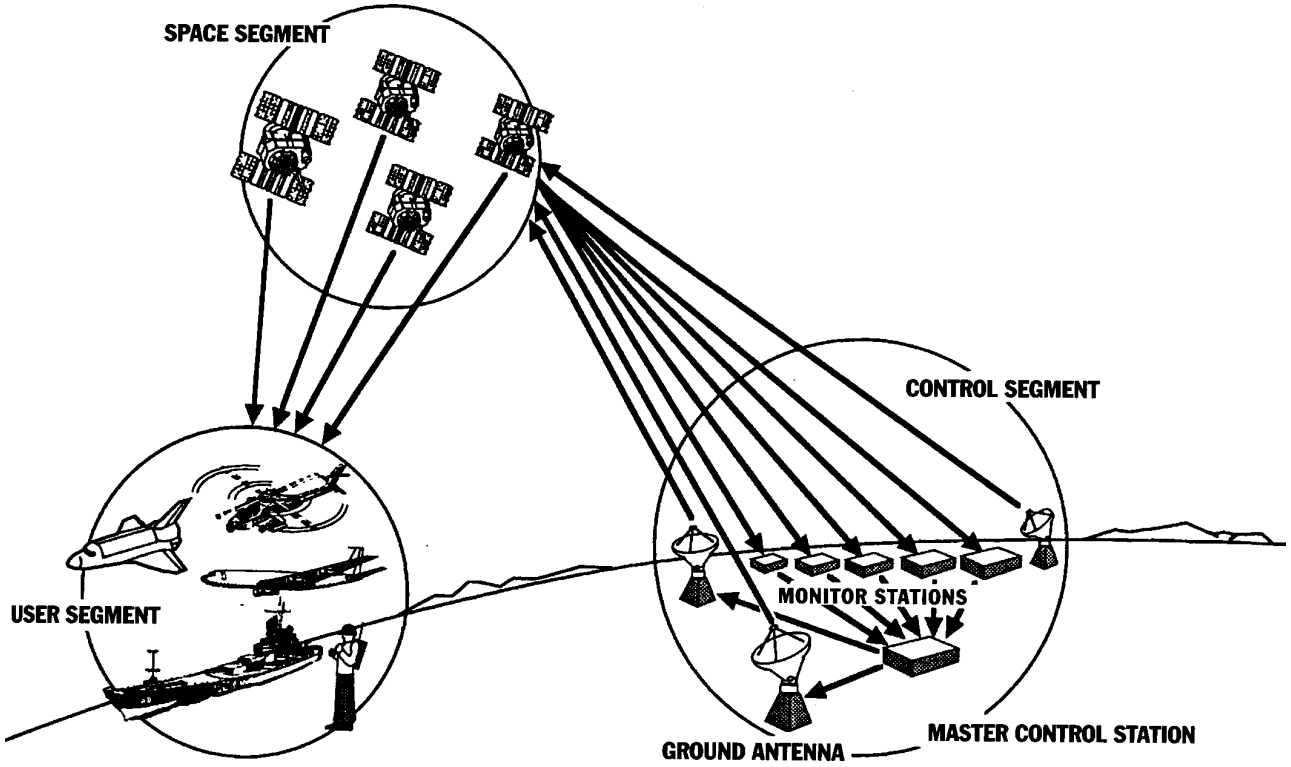
Various Systems



From: http://www.insidegnss.com/node/648

Technische Universität Berlin
Flugführung
und Luftverkehr

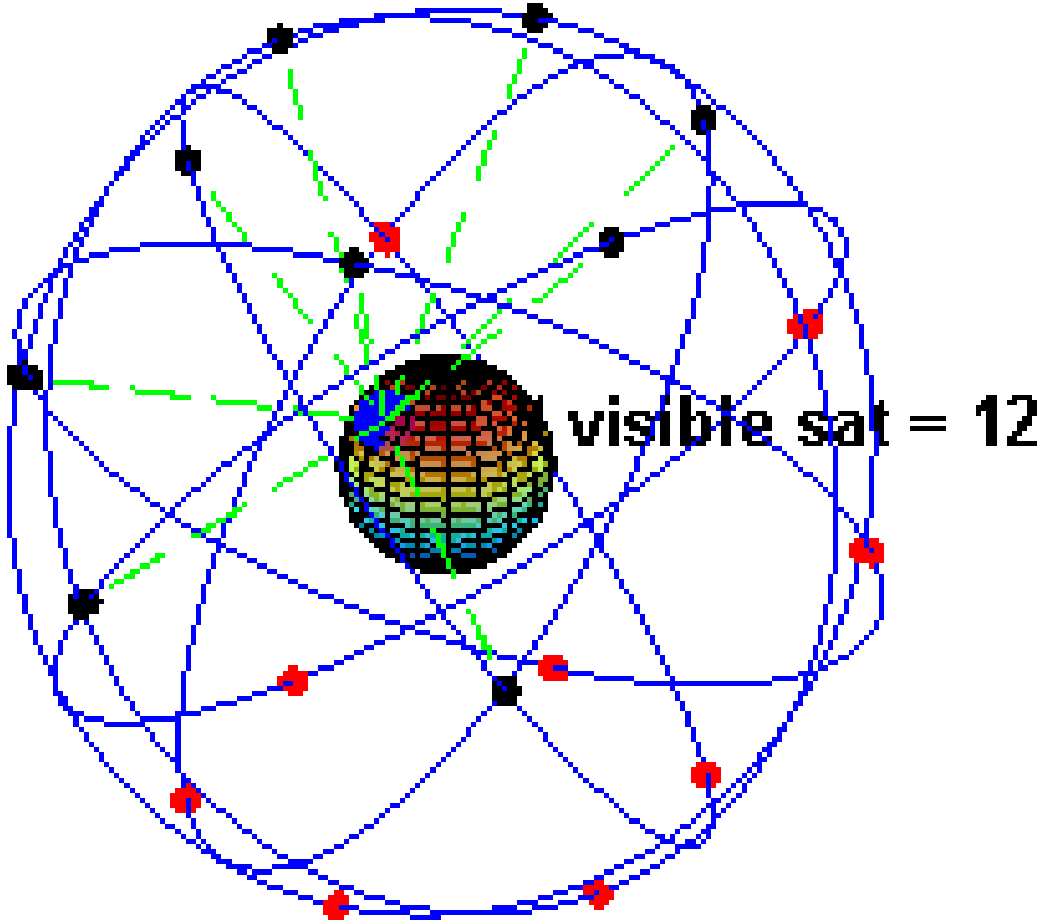
Three Segments of a GNSS System



- **Space**: the satellites themselves
- **Control**: monitors and controls satellites, generates ephemeris (and other) data
- **User**: anything that receives the GPS signal

Technische Universität Berlin
Flugführung und Luftverkehr

Global Positioning System (GPS) Example



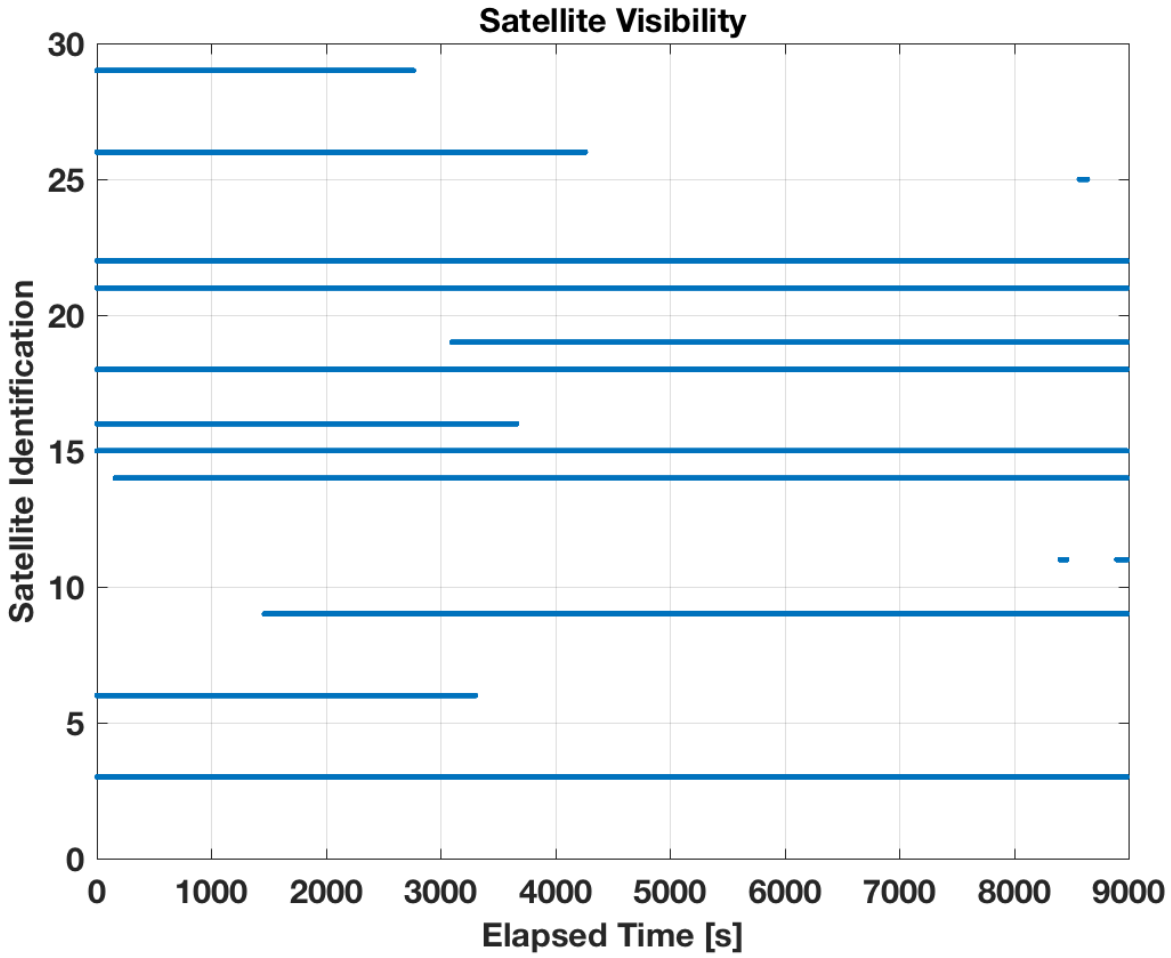
http://en.wikipedia.org/wiki/File:ConstellationGPS.gif

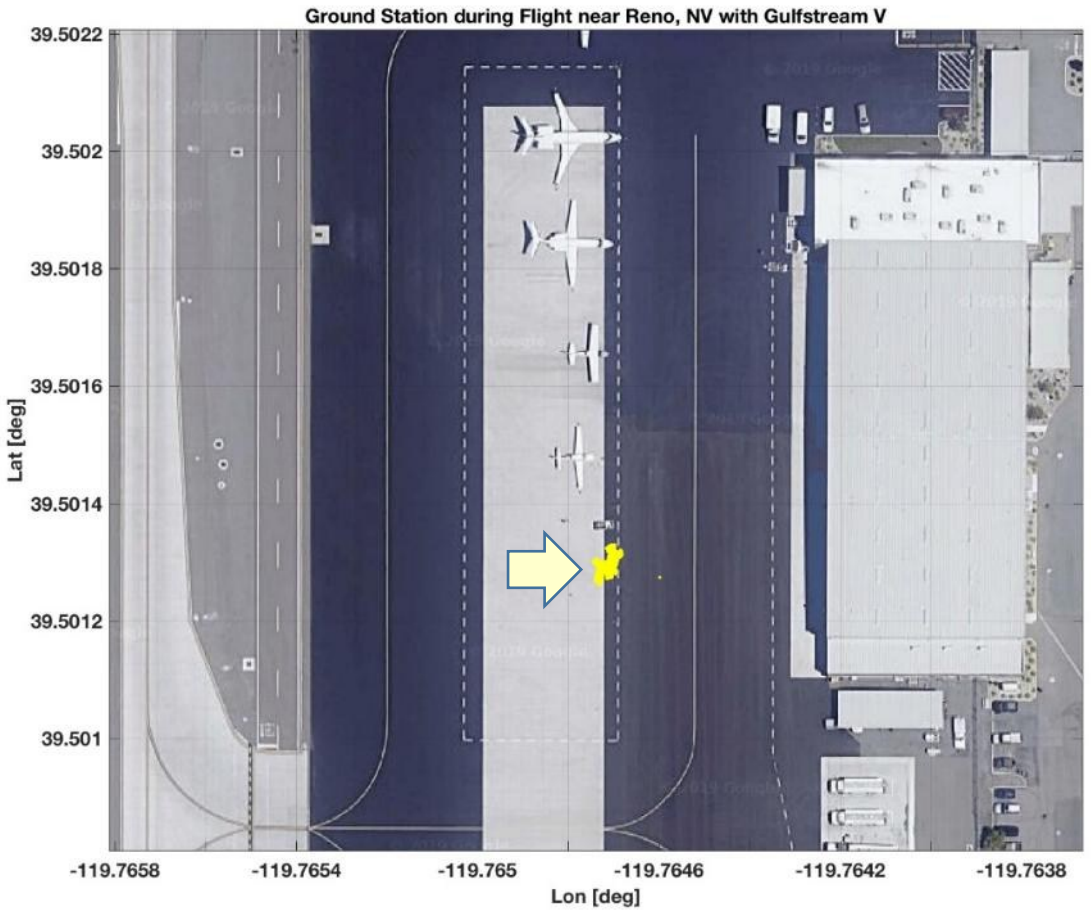
- 24 Satellites in 6 orbital planes inclined at 55 degrees with respect to the equatorial plane;
- Currently 26 satellites
- Repeating ground tracks - 23 hr 56 min;
- At least 4 satellites in view to a user;
- Anywhere on the Earth (7.5 on the average);
- Continuous, all-weather coverage;
- Orbit altitude is ~20,200 km (10,900 nmi) relative to the earth surface.

http://www.navcen.uscg.gov/
http://gps.gov

Technische Universität Berlin
Flugführung und Luftverkehr

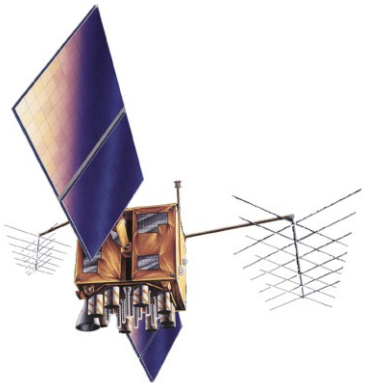
Satellite Visibility





Real stationary data collected during a flight test with a Gulfstream V at Reno, NV

GNSS Signal Structure – General Expression



$$s_{tx,j}(t) = A_{tx,j} G_j(t) D_j(t) \sin(2\pi f_{tx} t + \alpha_j)$$

Carrier-frequency

Transmitted signal

Transmitted signal amplitude

represents the transmitted spreading code, used to synchronize the received and locally generated signal (in receiver)

Navigation message data

Carrier signal

SV Carrier-Phase Offset

GNSS Control Segment

$$PR_j = \sqrt{(x_u - x_j)^2 + (y_u - y_j)^2 + (z_u - z_j)^2} + \delta t_u$$

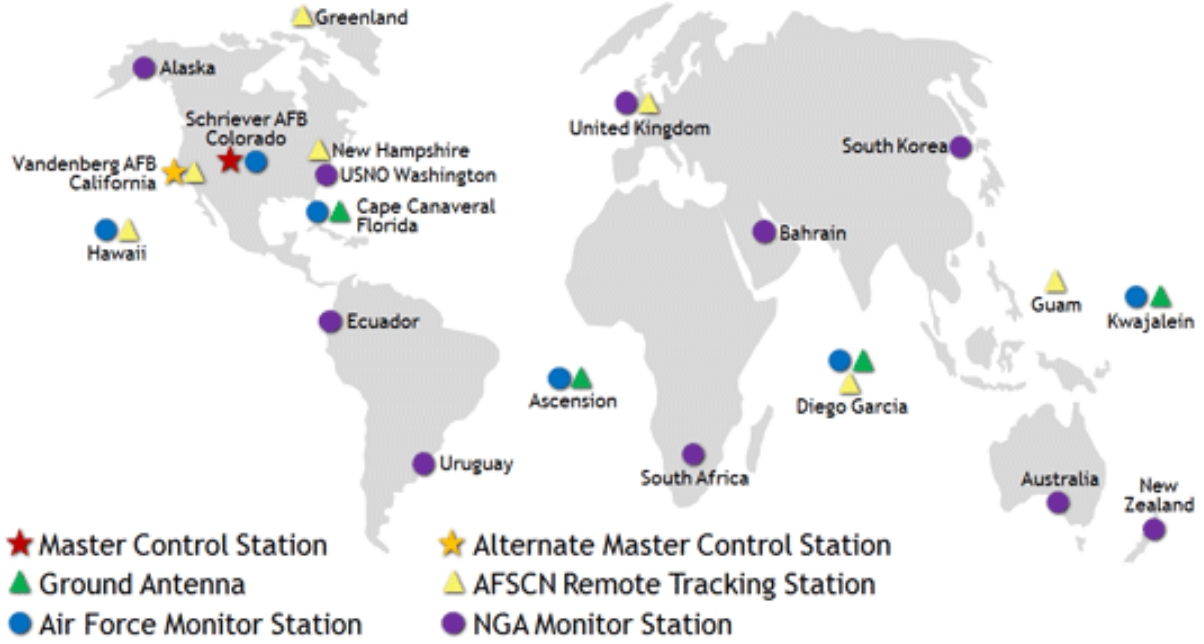
- Manages constellation (flies the satellites)
- Monitors GNSS system performance
- Calculates data sent over the **navigation message**
- **Navigation message contains parameters (trajectory model) so you can determine where the satellite is/was**

$$s_{tx,j}(t) = A_{tx,j} G_j(t) D_j(t) \sin(2\pi f_{tx} t + \alpha_j)$$

- Ground Control station(s) communicates with satellite using, for example, S-band data link (intermittent)
- Other name for satellites: **Space Vehicles** (SV)

Technische Universität Berlin
Flugführung und Luftverkehr

GPS Control Segment Example

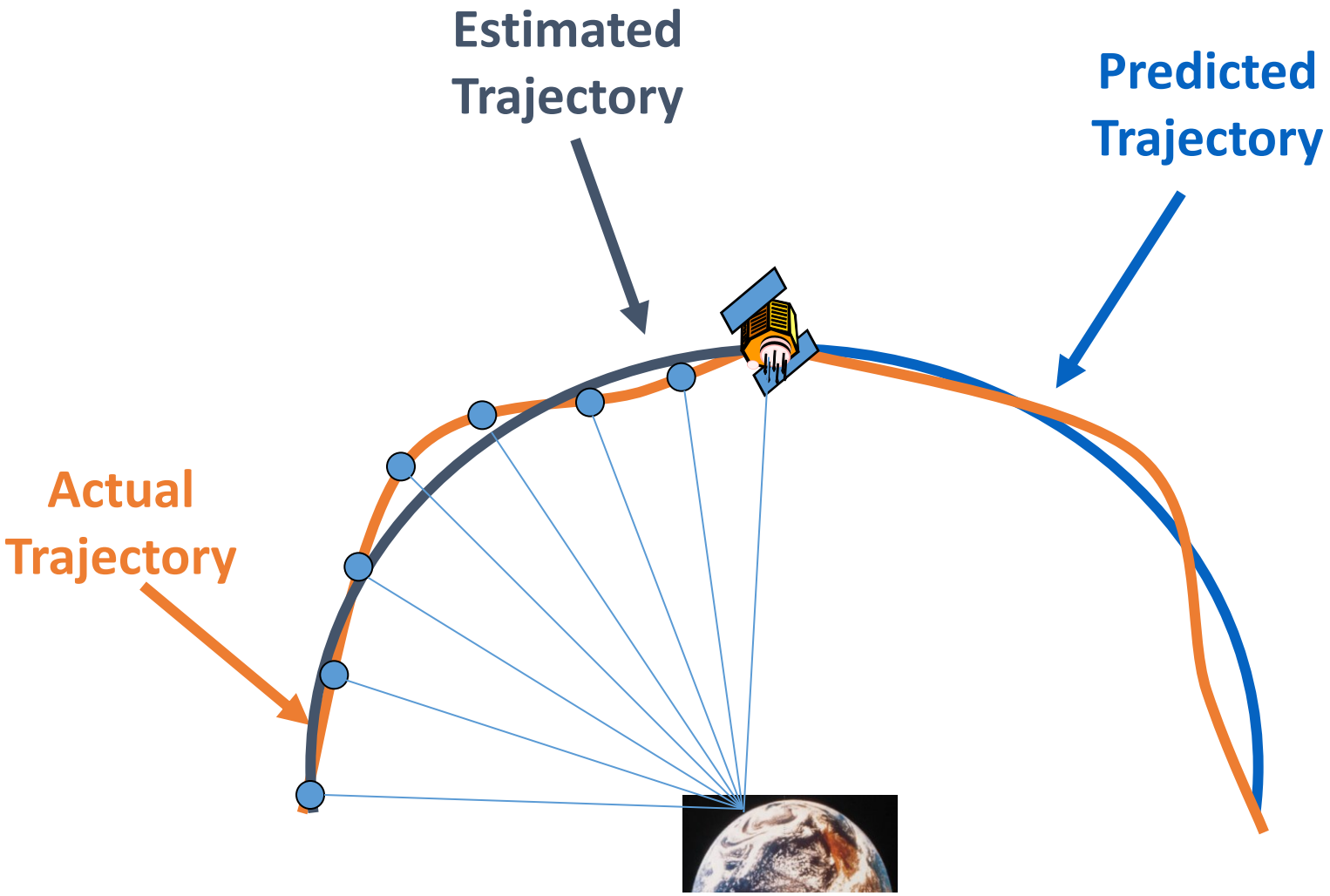


http://www.gps.gov

https://gssc.esa.int/navipedia/index.php?title=File:Galileo_Global_Ground_Segment.jpg

Technische Universität Berlin
Flugführung und Luftverkehr

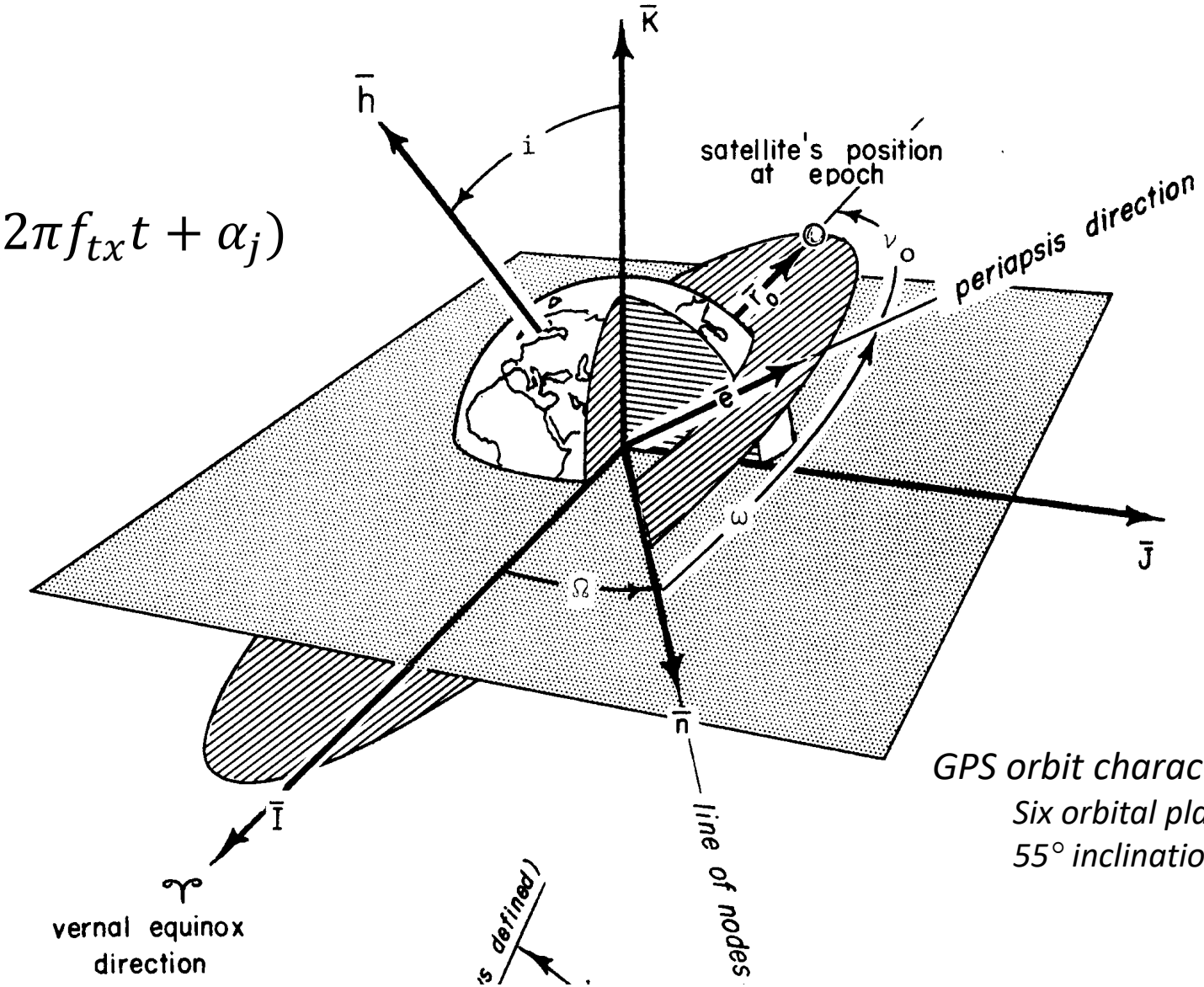
Satellite Trajectory Estimation and Prediction



Technische Universität Berlin
Flugführung und Luftverkehr

GNSS Ephemeris Data – Parameters

$$s_{tx,j}(t) = A_{tx,j} G_j(t) D_j(t) \sin(2\pi f_{tx} t + \alpha_j)$$

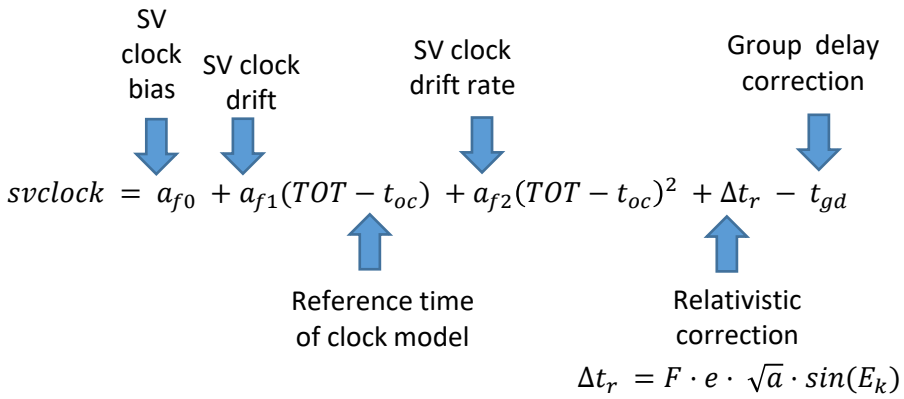


GPS orbit characteristics:
Six orbital planes
55° inclination angle

Technische Universität Berlin
Flugführung und Luftverkehr

GNSS Ephemeris Data – Clock Model

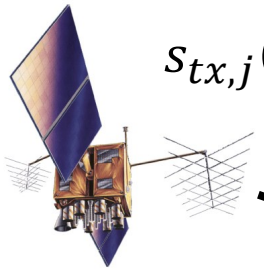
- Even though the GNSS satellites are clock synchronized, each satellite's clock deviates just a little bit from GNSS time.
- This difference must be corrected; therefore, the ephemerides also include clock model parameters:
  - A clock bias term
  - A clock drift and drift rate term
  - A relativity correction (since the in-orbit clock is accelerating)
  - A group delay due to delays in the instrumentation



Technische Universität Berlin
Flugführung und Luftverkehr

GNSS Received Signal Power (Link Budget)

$$s_{tx,j}(t) = A_{tx,j} G_j(t) D_j(t) \sin(2\pi f_{tx} t)$$



Transmit
For example, GPS L1:
478.63 W = 26.8 dBW

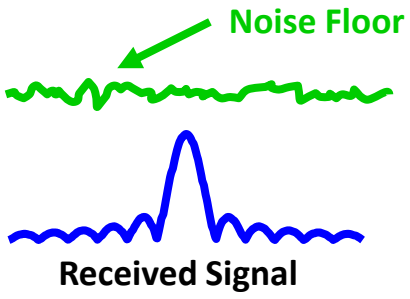
line-of-sight

Free Space Loss: -182.4 dB

Atmospheric Loss: -4.4 dB

Total loss: -186.8 dB (= $10^{-18.68}$)

Thermal Noise
(2 MHz Bandwidth):
10^{-14} W = -140 dBW



Received Signal:
10^{-16} W = -160 dBW

GNSS Receiver

- Power in dBW = $10\log_{10}$ (Power in W)
- Power in dBm = $10\log_{10}$ (Power in mW)
- 1 mW = 0.001 W = 0 dBm = -30 dBW

Institute of Aeronautics and Astronautics
Chair of Flight Guidance and Air Transport

Technische Universität Berlin
Flugführung und Luftverkehr

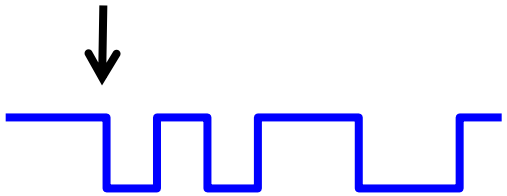
Timing in Signal

Transmitter side:

Time-of-Transmission (TOT) is encoded on the signal (signal contains a copy of the time-of-transmission in navigation data)

Receiver (user) side:

Time-of-Transmission (TOT)



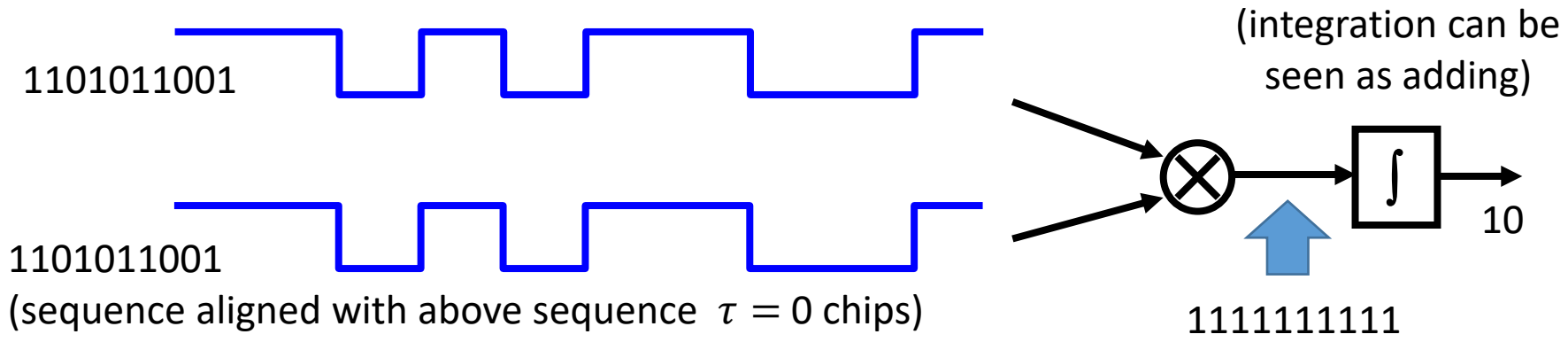
Estimated Range = (TOR – TOT)*(speed of the signal)

Time-of-Reception (TOR)

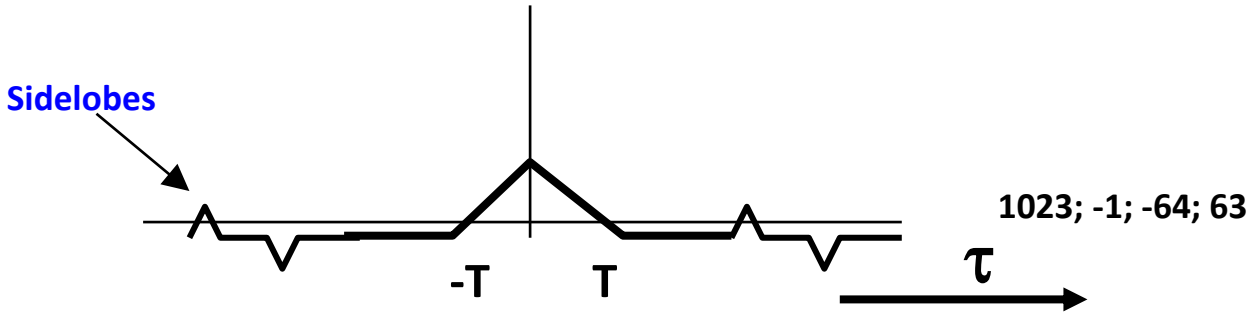
To find the TOT accurately, you need to know where the TOT is located by synchronizing the received signal with a local copy

Synchronization using Correlators

- Example:



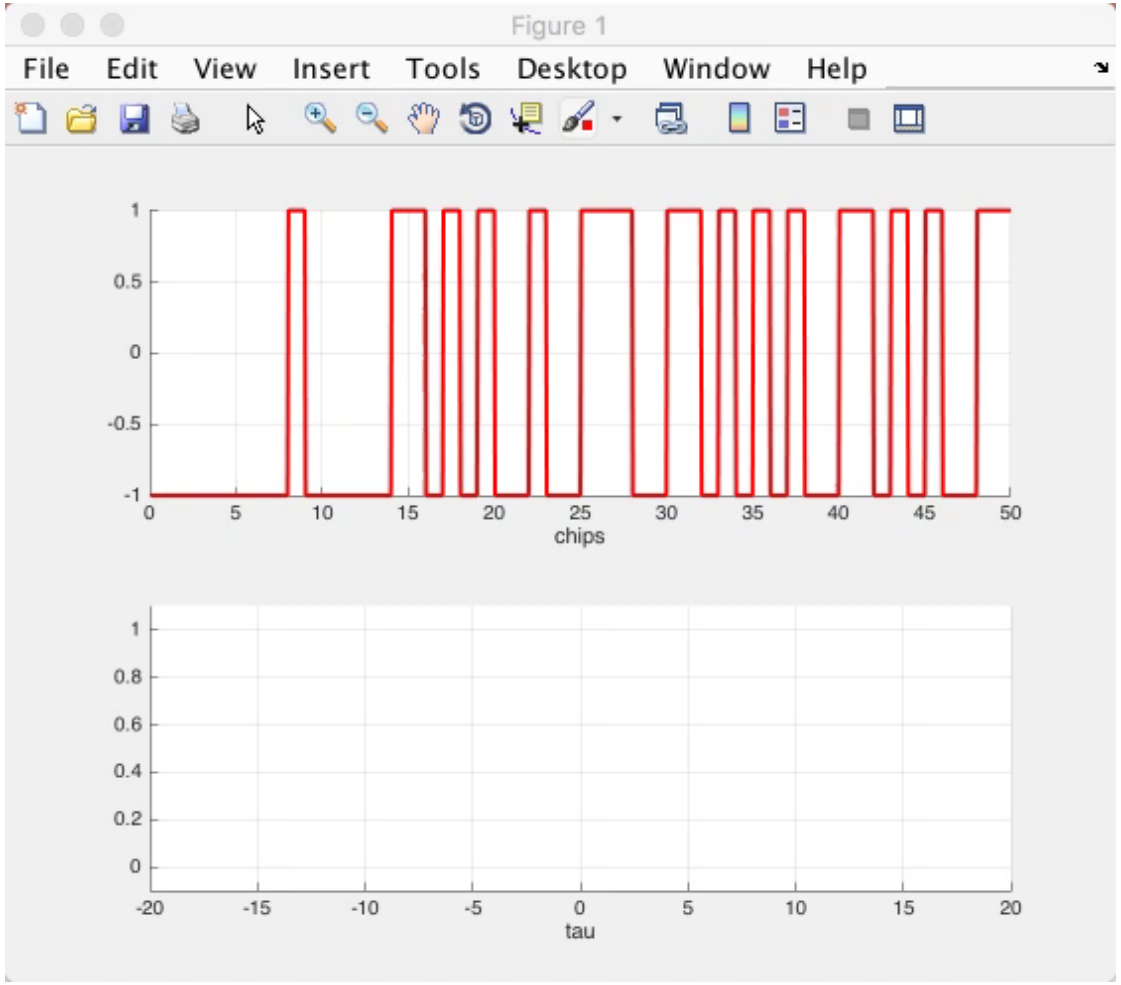
- For GPS PRN code (for various alignments, τ)

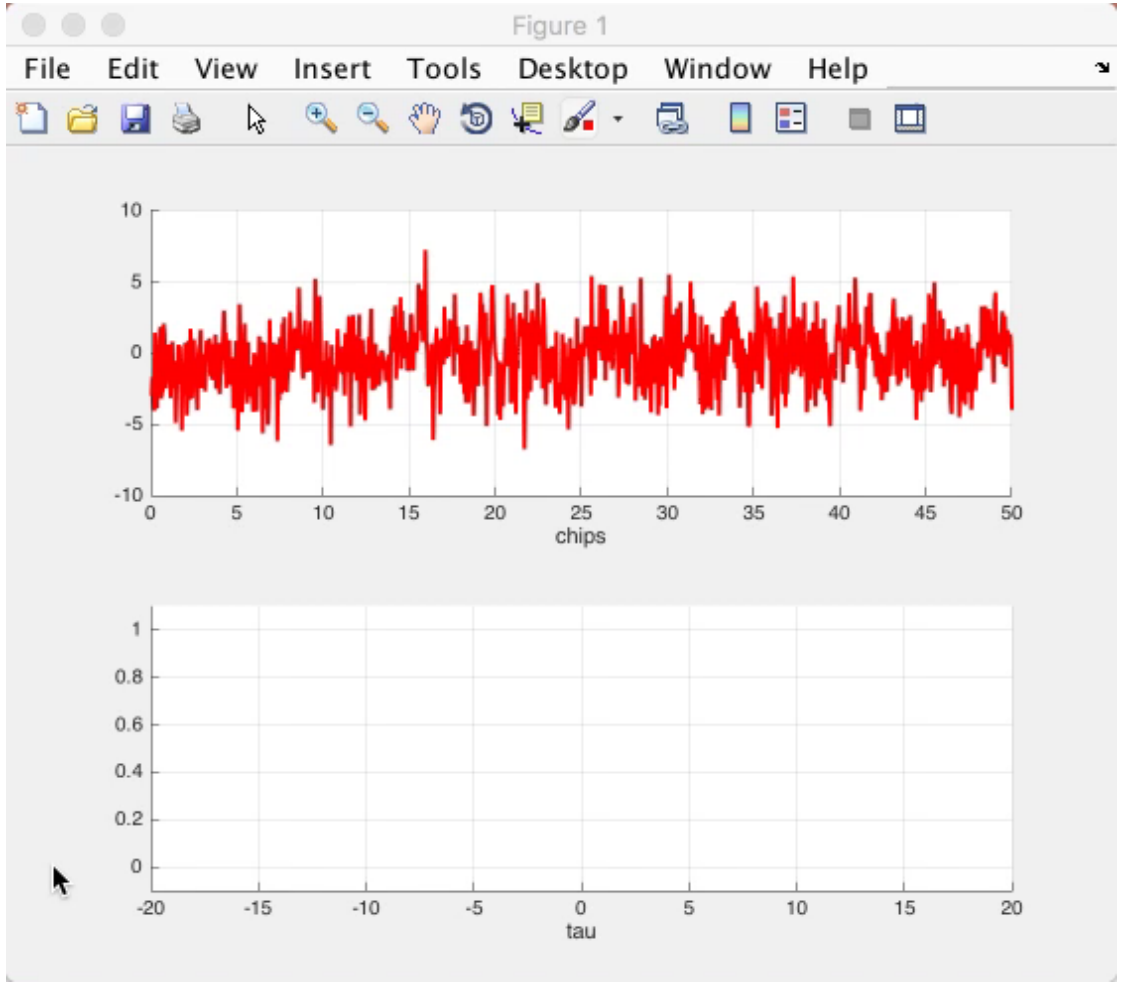


- Correlation is maximum when the two PRNs are aligned

GPS Cross-correlation Animation

Technische Universität Berlin
Flugführung und Luftverkehr

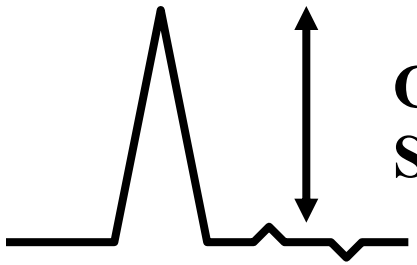




Technische Universität Berlin
Flugführung und Luftverkehr

GNSS Cross-correlation

- Cross-correlation is the key to GNSS operation:
  - The received signal is below the noise floor.
  - The correlator allows the receiver the align a locally-generated code with the incoming code.
  - Integration over all chips increases the received signal power.
    The noise; however, is reduced.

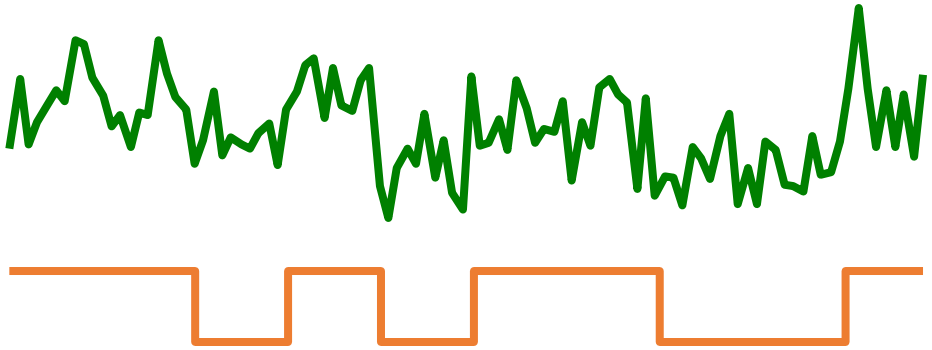


GPS example: Correlation
Sidelobes are at least 22dB down

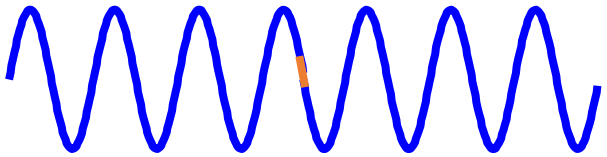
Technische Universität Berlin
Flugführung und Luftverkehr

“Raw” Measurements

- Code-phase measurement or pseudorange (e.g., C/A)



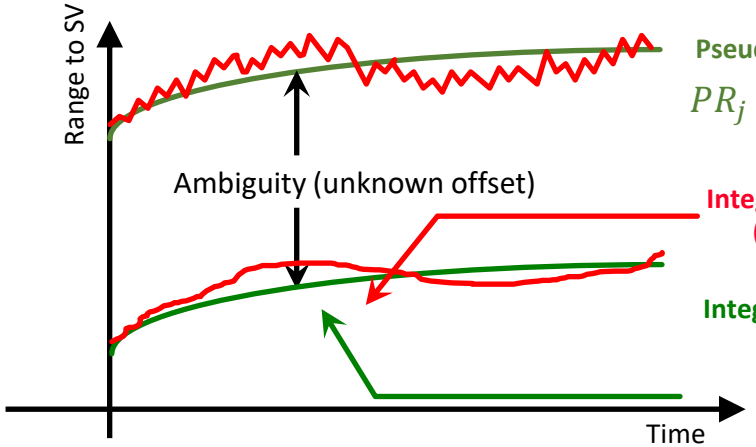
- Carrier-phase measurement or integrated Doppler frequency shift (also referred to as accumulated Doppler shift)



	Pseudorange	Carrier-Phase
Type of measurement	Range (absolute)	Range (ambiguous)
Measurement precision	dm-level	mm-level
Robustness	More robust	Less robust (cycle slips possible)

Technische Universität Berlin
Flugführung und Luftverkehr

“Raw” Measurements



$$PR_j = R_j + c\delta t_u + \delta R_{PR}$$

Pseudorange (measured)

Pseudorange (true)

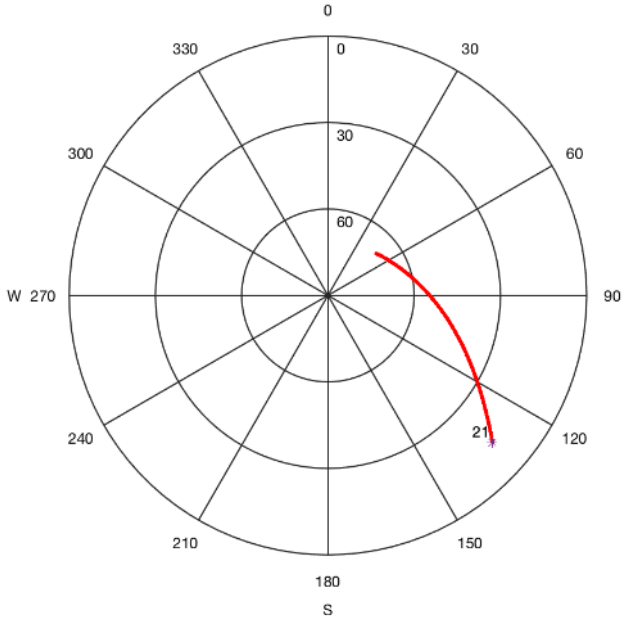
$$PR_j = R_j + c\delta t_u$$

Integrated Doppler (measured)

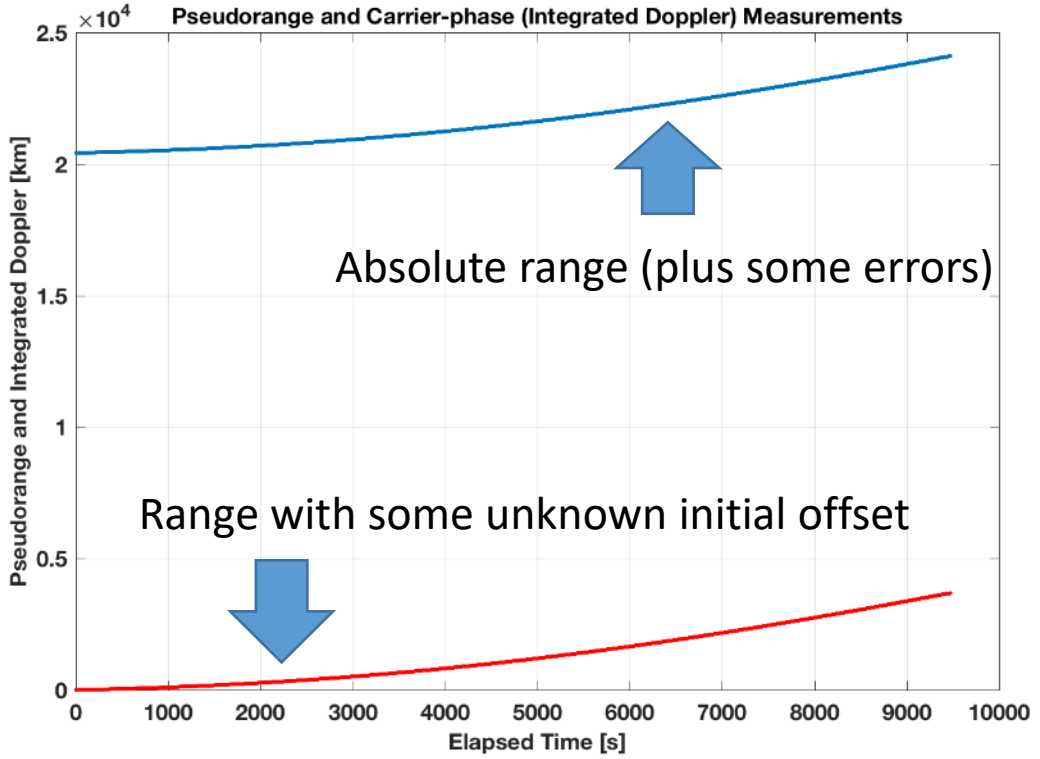
$$\phi_j = R_j + \boldsymbol{N_j\lambda} + c\delta t_u + \delta R_{ID}$$

Integrated Doppler (true)

$$\phi_j = R_j + \boldsymbol{N_j\lambda} + c\delta t_u$$



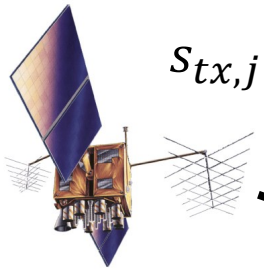
Satellite starts at an elevation of about 70 degrees and drops to an elevation of about 10 degrees



Institute of Aeronautics and Astronautics
Chair of Flight Guidance and Air Transport

Technische Universität Berlin
Flugführung und Luftverkehr

Received Signal – Doppler Frequency

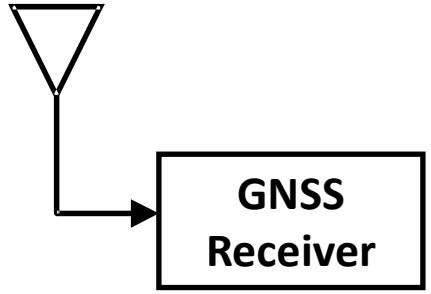


$$s_{tx,j}(t) = A_{tx,j} G_j(t) D_j(t) \sin(2\pi f_{tx} t + \phi_j)$$

line-of-sight dynamics causes a Doppler frequency that is a function of the carrier-frequency and the line-of-site rate

$$\Delta f = -\frac{\mathbf{v} \cdot \mathbf{e}_j}{c} f_{tx}$$

$$s_{rx,j}(t) = \alpha_j A_{tx,j} G_j(t) D_j(t) \sin(2\pi [f_{tx} + \Delta f] t + \phi_j)$$

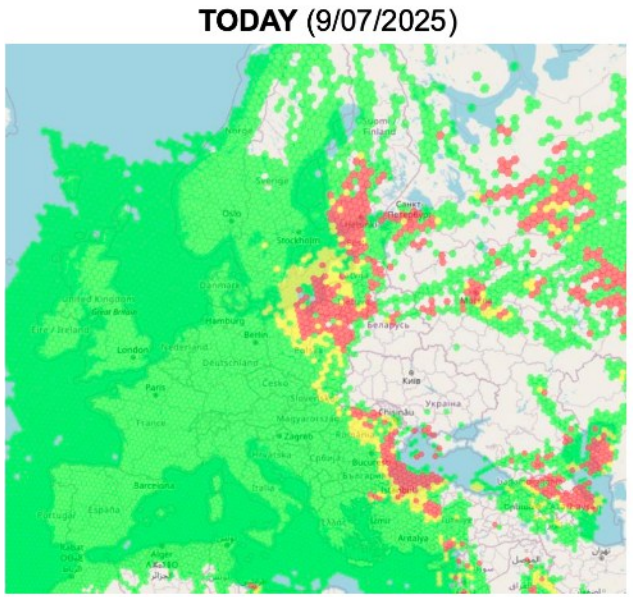


$\mathbf{v}$: relative 3D velocity of the GNSS receiver (user) with respect to the satellite
c: speed of light

Technische Universität Berlin
Flugführung und Luftverkehr

Pseudorange and Carrier-Phase Errors

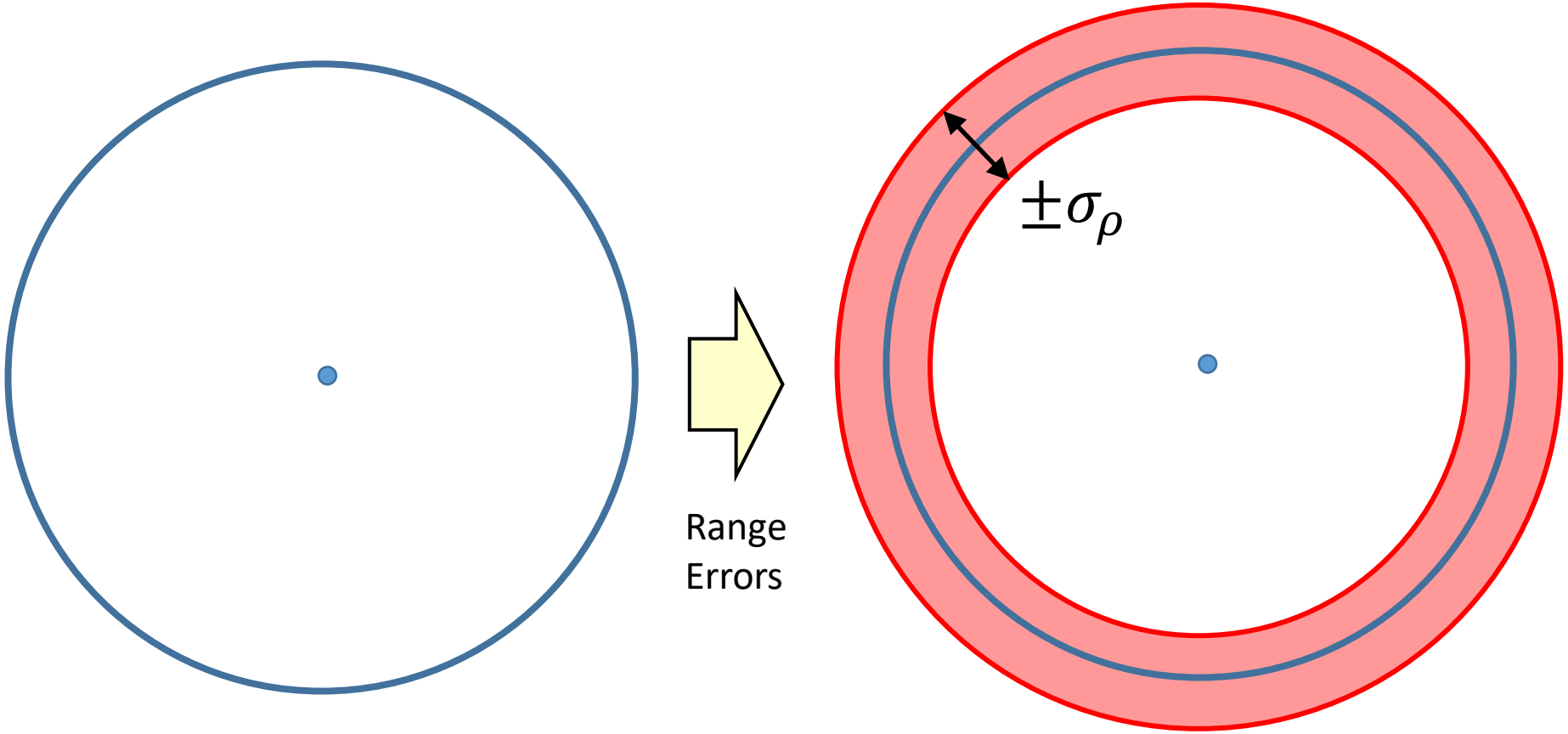
- Major error sources
  - Propagation delays (ionosphere, troposphere)
  - Satellite orbit and clock errors
  - Receiver measurement errors (noise + dynamics)
  - Multipath (diffuse and specular)
- Others:
  - Interference/jamming
  - Spoofing
  - None-Line-of-sight



Source: Gpsjam.org

Graphical Interpretation of Range Error

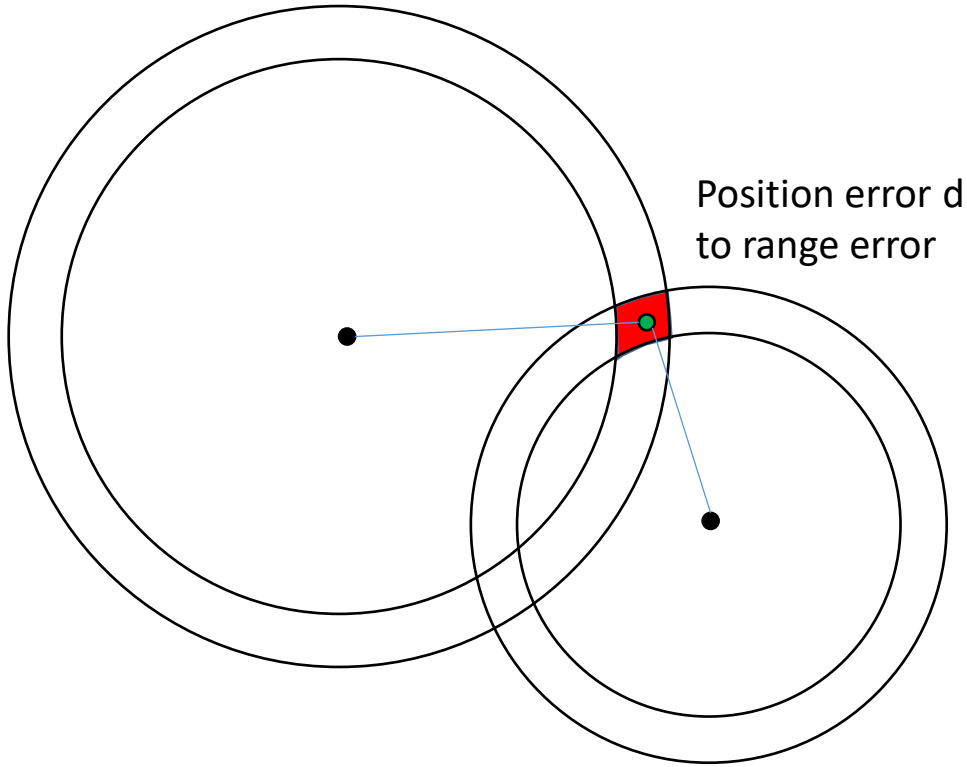
Technische Universität Berlin
Flugführung und Luftverkehr



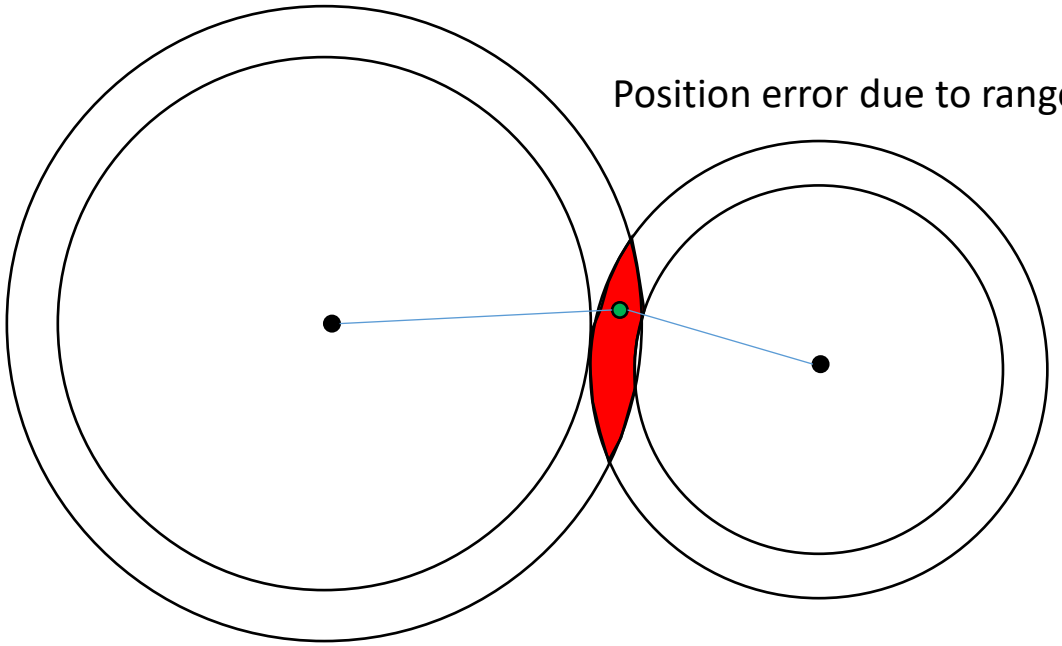
Graphical Interpretation: Geometry

Technische Universität Berlin
Flugführung und Luftverkehr

Good geometry



Bad geometry



Larger position error due to worse geometry


Questions?

GNSS Signal Structure – GPS L1 Example

Carrier-frequency
1575.42 MHz

$$s_{tx,G,L1,j}(t) = A_{tx,G,L1,j} G_j(t) D(t) \sin(2\pi f_{L1} t + \alpha_j)$$

Transmitted signal amplitude

Navigation Message data at 50 bps

Carrier signal

SV Carrier-Phase Offset

represents the C/A code (+1 or –1), a pseudo-random noise (PRN) code transmitted at a rate of 1.023 Mcps (chips per second) and repeated every 1 ms (i.e., 1023 chips)

Measurement Equation

Technische Universität Berlin
Flugführung und Luftverkehr

Difference between user clock and satellite clock (here in meters)

GNSS Satellite position

$$\mathbf{z} = \begin{bmatrix} PR_1 \\ PR_2 \\ \vdots \\ PR_N \end{bmatrix} = \mathbf{h}(\mathbf{x}) = \begin{bmatrix} \sqrt{(x_u - x_1)^2 + (y_u - y_1)^2 + (z_u - z_1)^2} + c\delta t_u \\ \sqrt{(x_u - x_2)^2 + (y_u - y_2)^2 + (z_u - z_2)^2} + c\delta t_u \\ \vdots \\ \sqrt{(x_u - x_N)^2 + (y_u - y_N)^2 + (z_u - z_N)^2} + c\delta t_u \end{bmatrix}$$

$$\Rightarrow \mathbf{z} = \begin{bmatrix} \|\mathbf{r}_u - \mathbf{r}_1\| + c\delta t_u \\ \|\mathbf{r}_u - \mathbf{r}_2\| + c\delta t_u \\ \vdots \\ \|\mathbf{r}_u - \mathbf{r}_N\| + c\delta t_u \end{bmatrix}$$

Use norm to express the distance

$\mathbf{r}_u$: user position
$\mathbf{r}_i$: satellite 'i' position

Technische Universität Berlin
Flugführung und Luftverkehr

PR and CP Error Equations

Pseudorange (PR):

$$PR_j = R_j + c\delta t_u + \delta R_{iono} + \delta R_{tropo} + \delta R_{PR,noise} + \delta R_{PR,mp} + \delta R_{PR,hw} - c\delta t_{SV,j}$$

- R_j: True geometric range
- $c\delta t_u$: User clock error
- δR_{iono}: Error due to delay in Ionosphere
- δR_{tropo}: Error due to delay in Troposphere
- $\delta R_{PR,noise}$: Error due to Thermal Noise
- $\delta R_{PR,mp}$: Error due to Multipath (Reflections)
- $\delta R_{PR,hw}$: Error due to Hardware Delays in Receiver
- $c\delta t_{SV,j}$: Satellite clock and orbit error

Carrier-Phase (CP):

$$\phi_j = R_j + N_j\lambda + c\delta t_u - \delta R_{iono} + \delta R_{tropo} + \delta R_{ID,noise} + \delta R_{ID,mp} + \delta R_{ID,hw} - c\delta t_{SV,j}$$

- $N_j\lambda$: Unknown offset
- $-\delta R_{iono}$: Opposite sign from PR
- $\delta R_{ID,noise}$: Much smaller noise (mm-level)
- $\delta R_{ID,mp}$: Smaller multipath (cm-level)