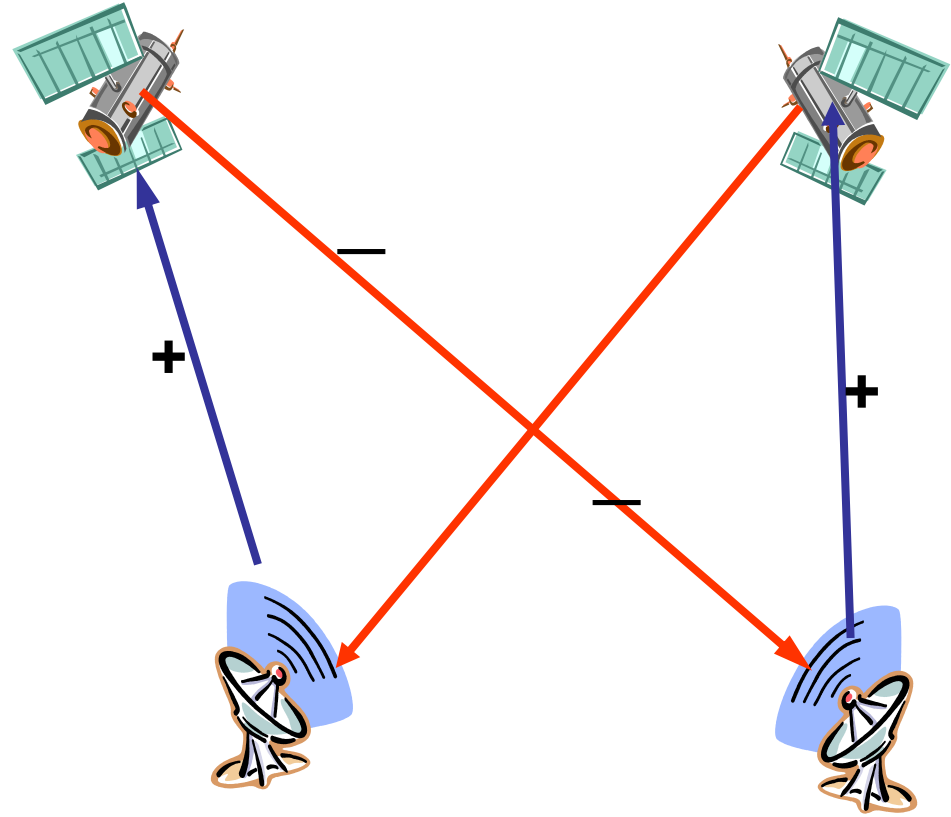
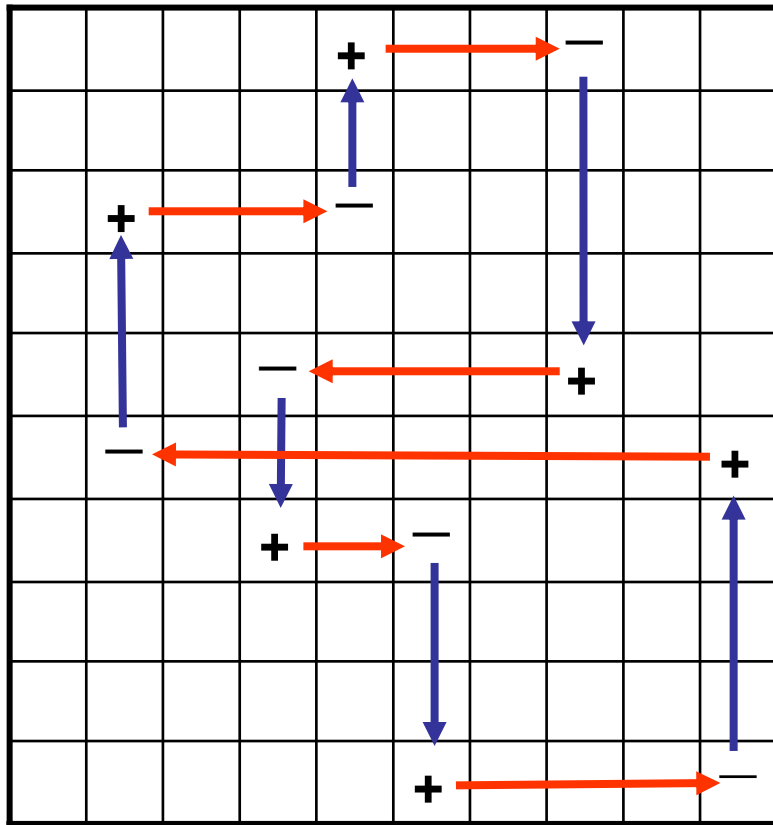


Plus-minus paths

Alan Saalfeld
Geodetic Science and Computer Science

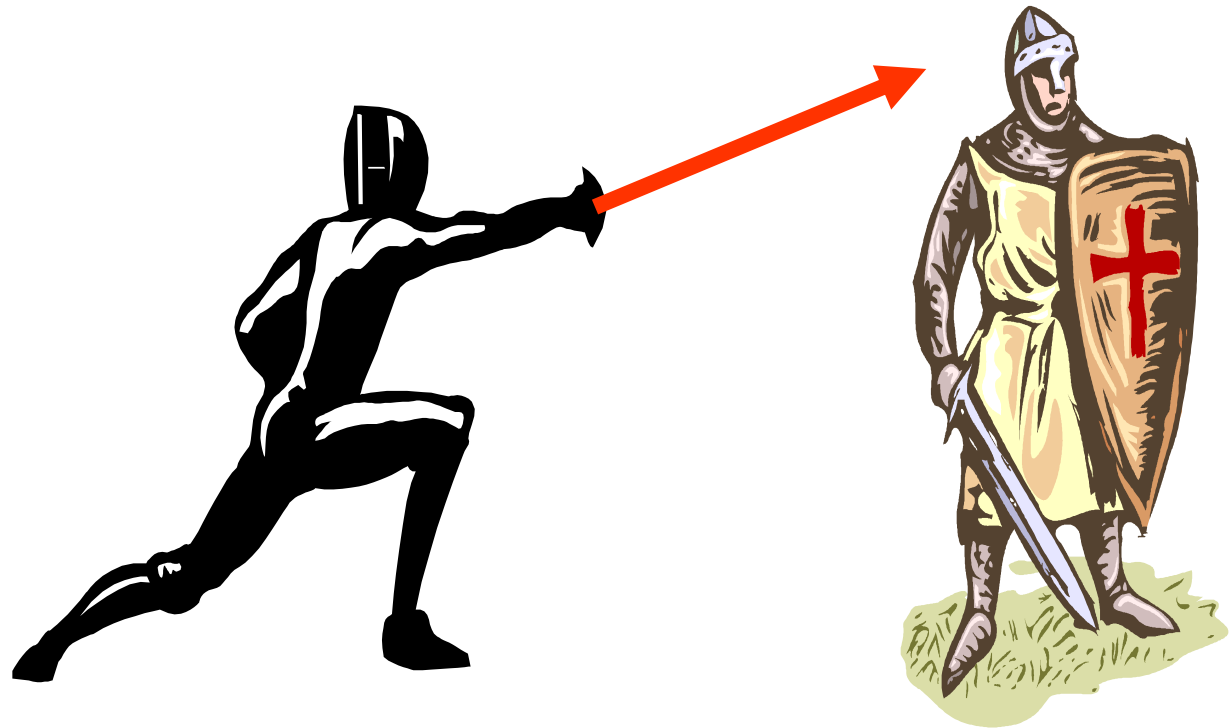


Two **Adversarial** Math Problems

- Historical overview
 - How the Global Positioning System works and how double differencing (plus-minus paths) made it work even better
 - How the US Census Bureau uses plus-minus paths to remove sensitive data from its published tables
- New insights that come from viewing the problems in a vector space framework

Math vs US DoD

- Math wins!
- The vector is mightier than the sword!



Geodesy Aptitude Quiz

Pick the best answer(s).

Time is:

- A. money.
- B. distance.
- C. location.

Geodesy Aptitude Quiz

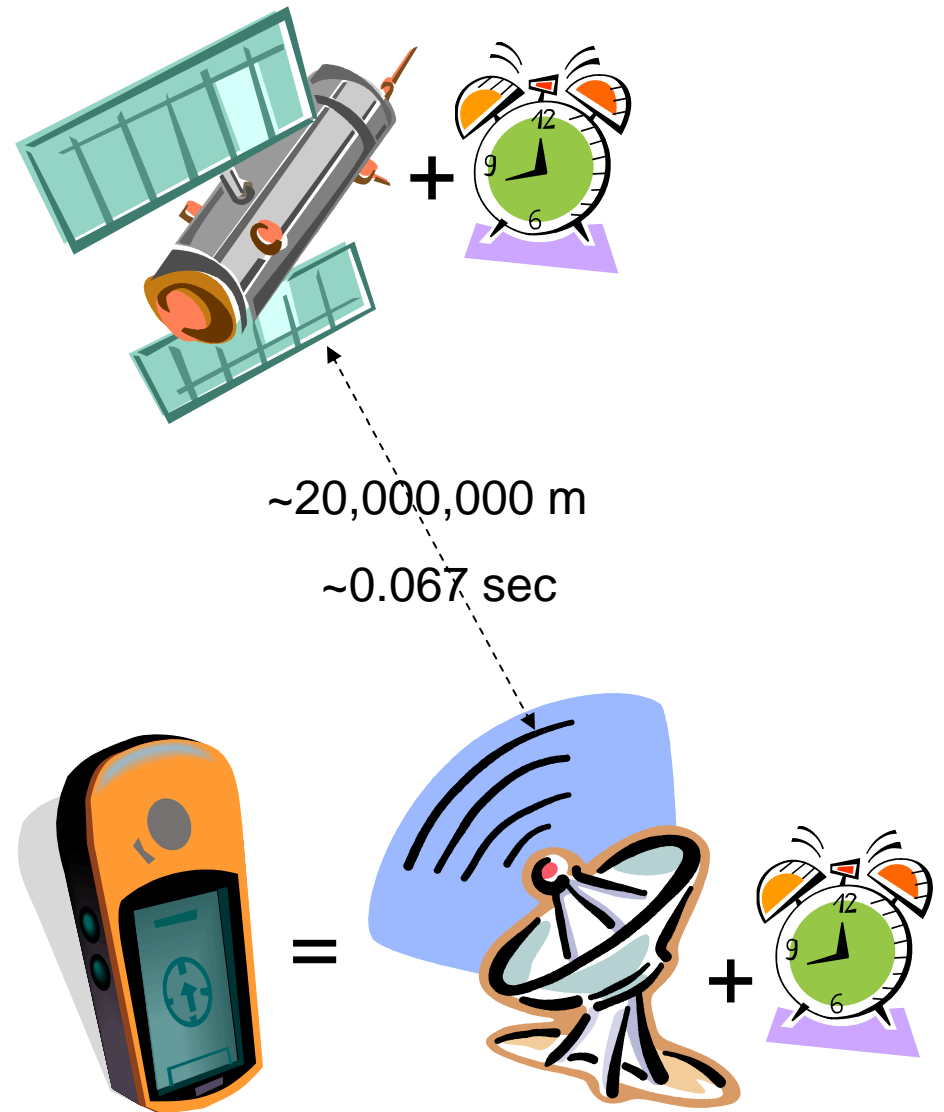
Answer key:

Time is:

- A. ~~money~~. Incorrect (or at least not true in academia!)
- B. distance. Correct (and that is what we will focus on today.)
- C. location. Also true in the history of geodesy—see Dava Sobel's book *Longitude* for more info.

How a GPS receiver works

- Satellites send signals at the speed of light (c)
- Time yields distance:
 $\text{time} = \text{distance}/\text{speed}$
- $c = 299\,792\,458$ m/sec or 0.3 m/nanosecond
- For 1-meter precision, clock must have 0.000000003-second or 3-nanosecond precision
- Clocks on satellite and receiver need to be synchronized



How is receiver position computed?

t^j = time that the satellite signal is sent by satellite j .

t_a^j = time that the satellite j 's signal is received by receiver a .

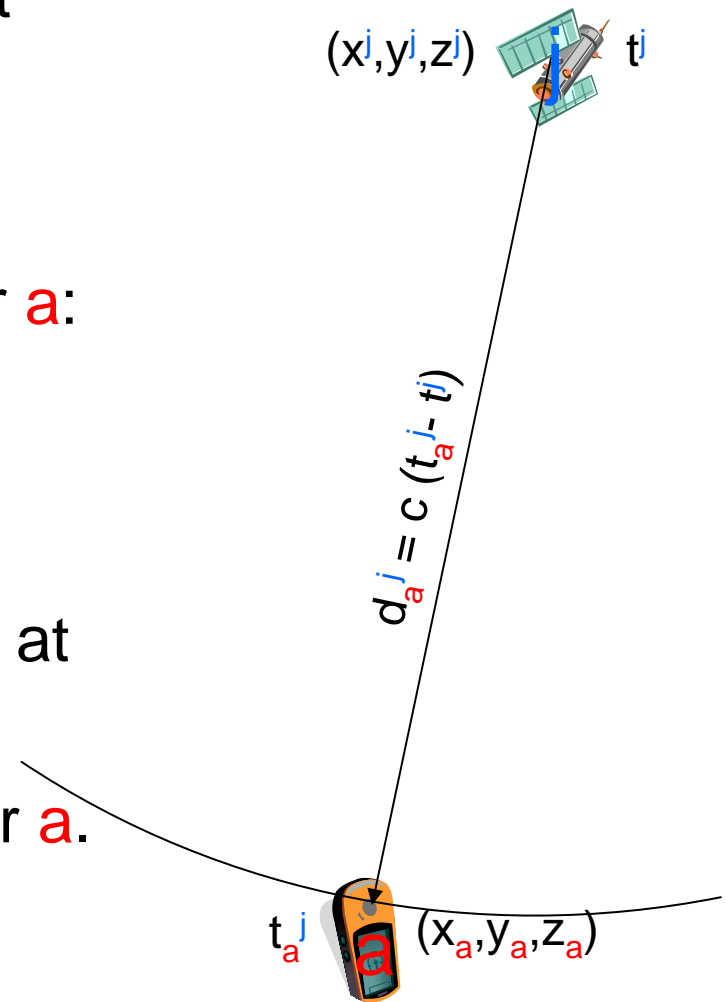
Distance d_a^j from satellite j to receiver a :

$$d_a^j = c (t_a^j - t^j).$$

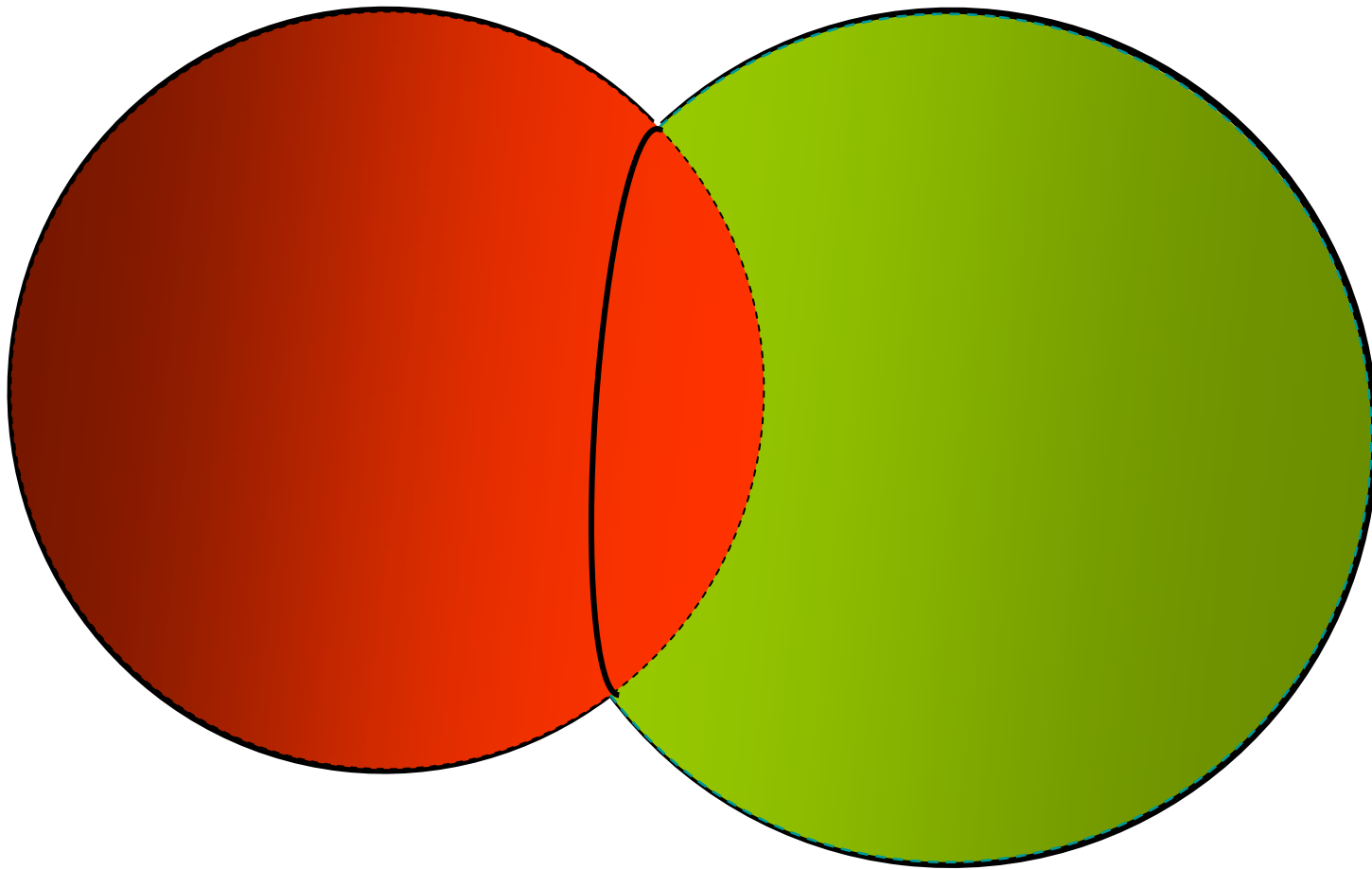
(x^j, y^j, z^j) is the position of the satellite j at time t^j .

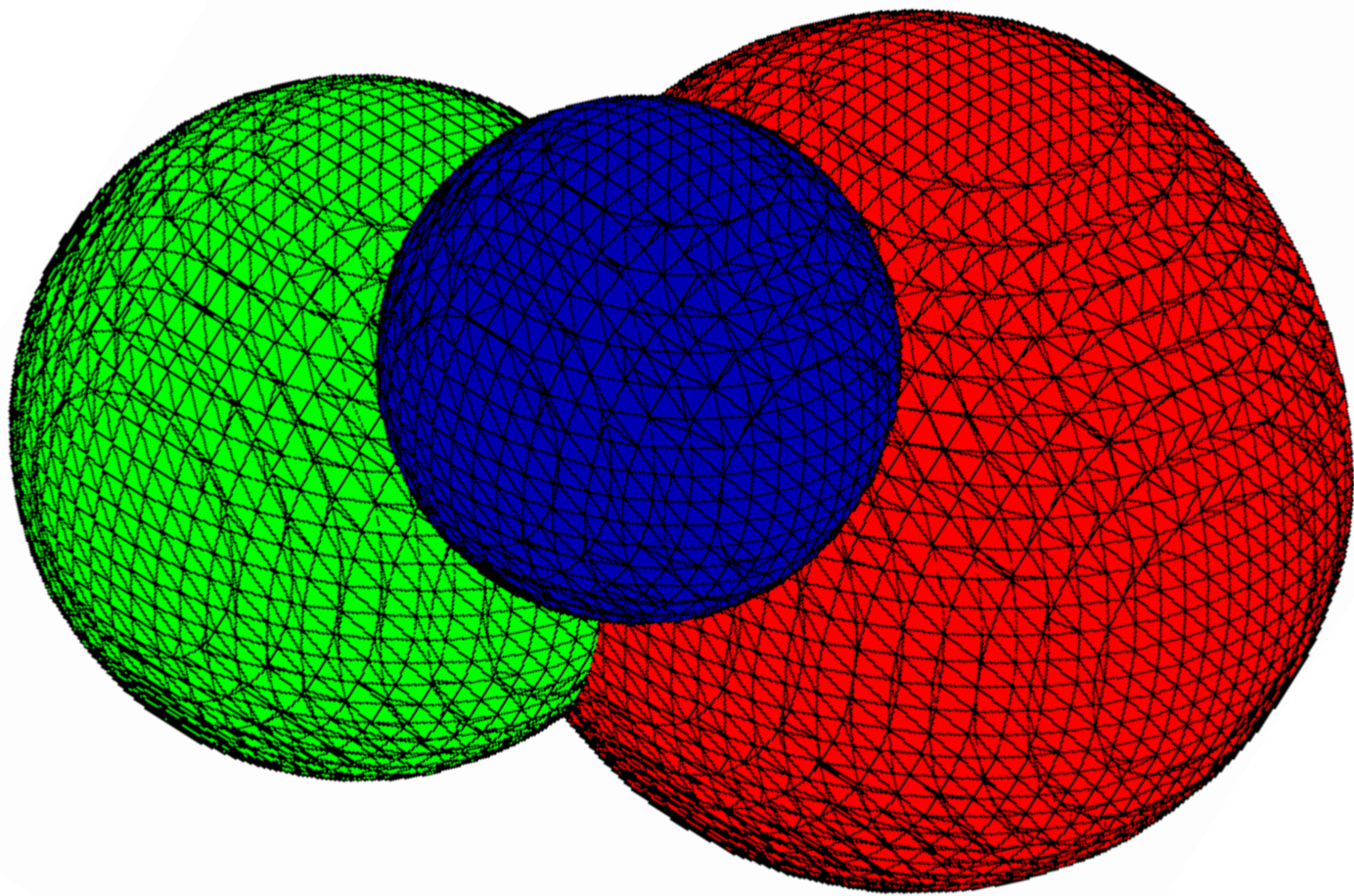
(x_a, y_a, z_a) is the position of the receiver a .

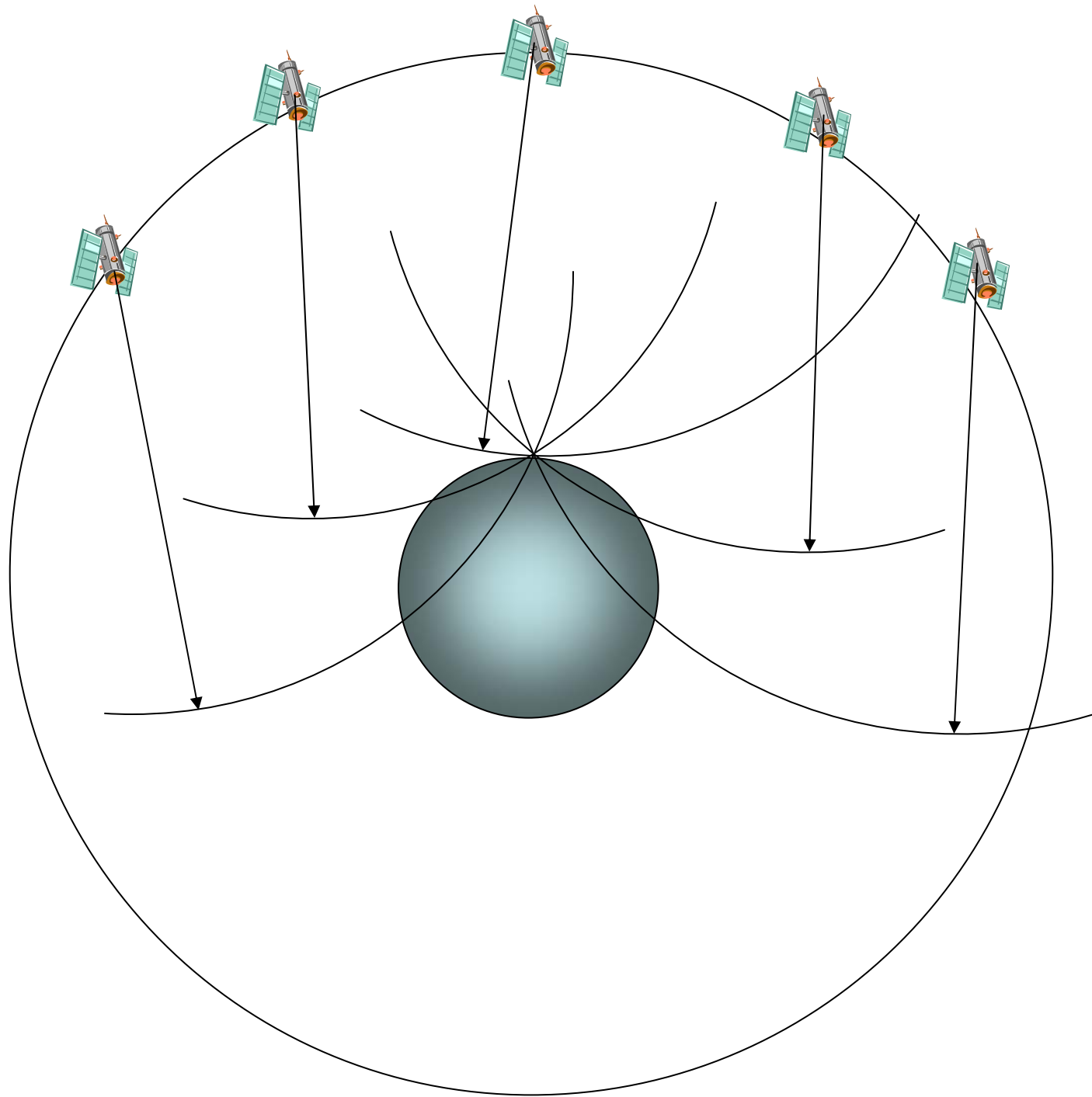
$$(d_a^j)^2 = (x^j - x_a)^2 + (y^j - y_a)^2 + (z^j - z_a)^2$$



Sphere Intersections







What if the clocks aren't correct?

True distance computations

t^j = time that the satellite signal actually is sent by satellite j .

t_a^j = time that the satellite j 's signal actually is received by receiver a .

Actual distance d_a^j from satellite j to receiver a :

$$d_a^j = c(t_a^j - t^j).$$

Recorded distance computations

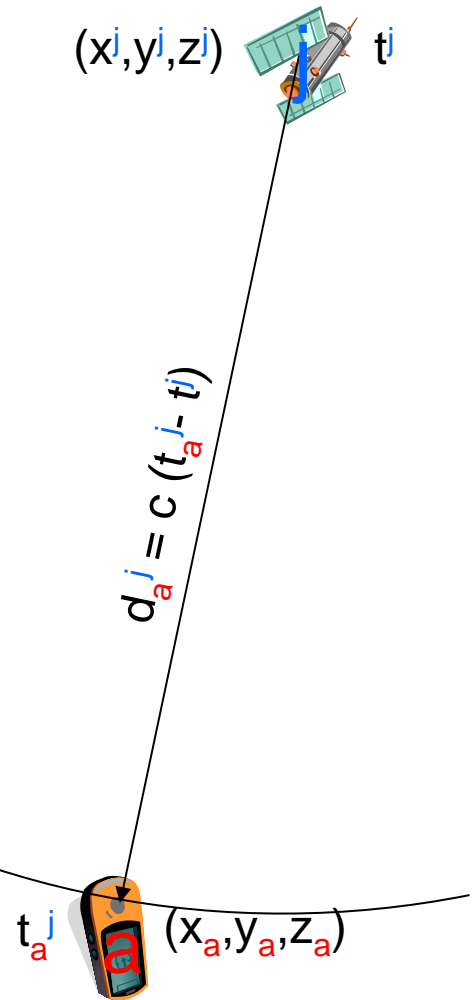
$T^j = t^j + e^j$ = time recorded for the satellite signal sending time by satellite j (e^j is the clock error of j).

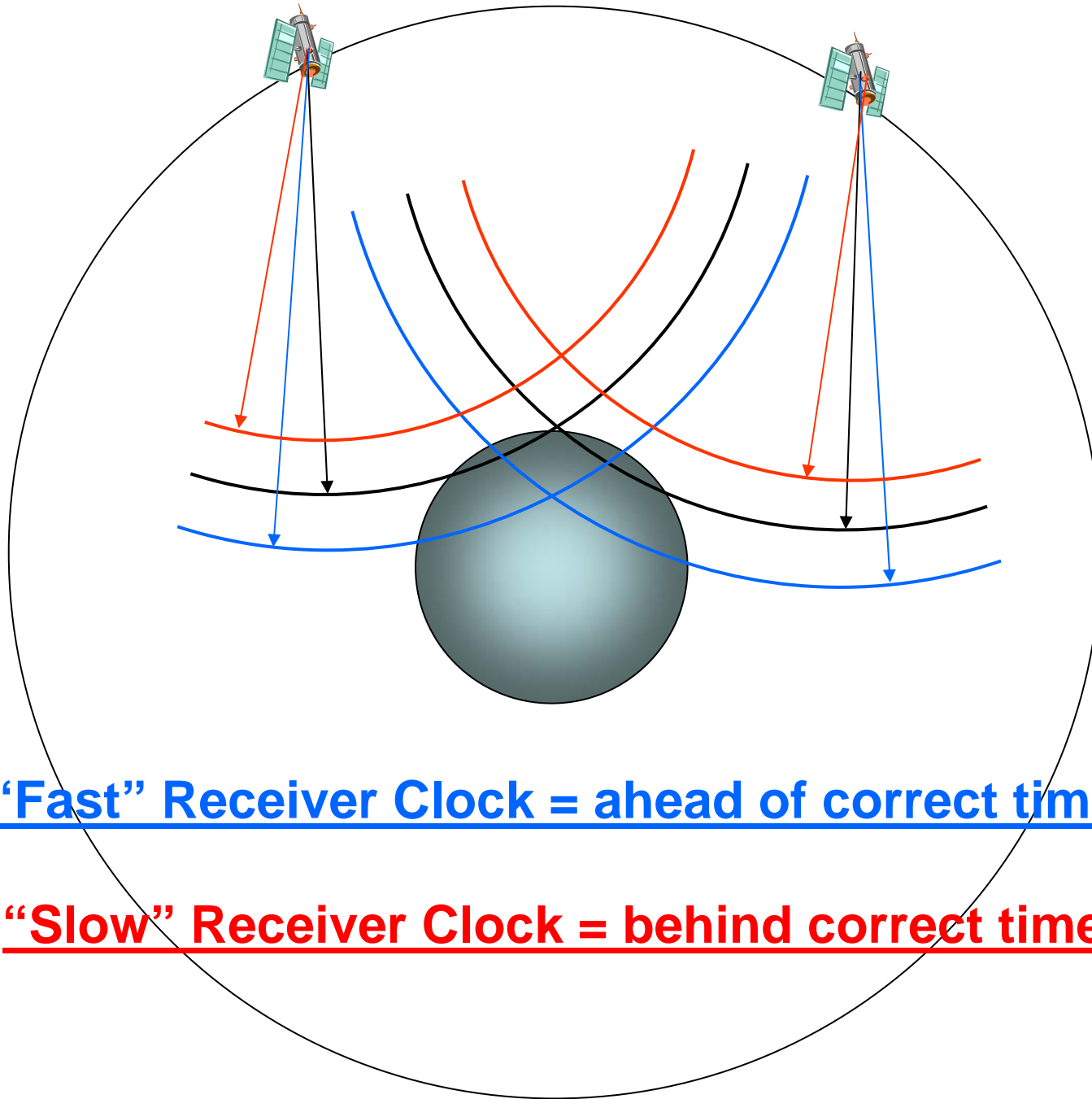
$T_a^j = t_a^j + e_a$ = time recorded for the satellite j 's signal receiving time by receiver a (a 's clock error is e_a).

Computed distance D_a^j from satellite j to receiver a :

$$D_a^j = c(T_a^j - T^j) = c(t_a^j - t^j) + c(e_a - e^j) = d_a^j + c(e_a - e^j).$$

The total distance error $D_a^j - d_a^j = c(e_a - e^j)$ is proportional to clock error difference ($e_a - e^j$).

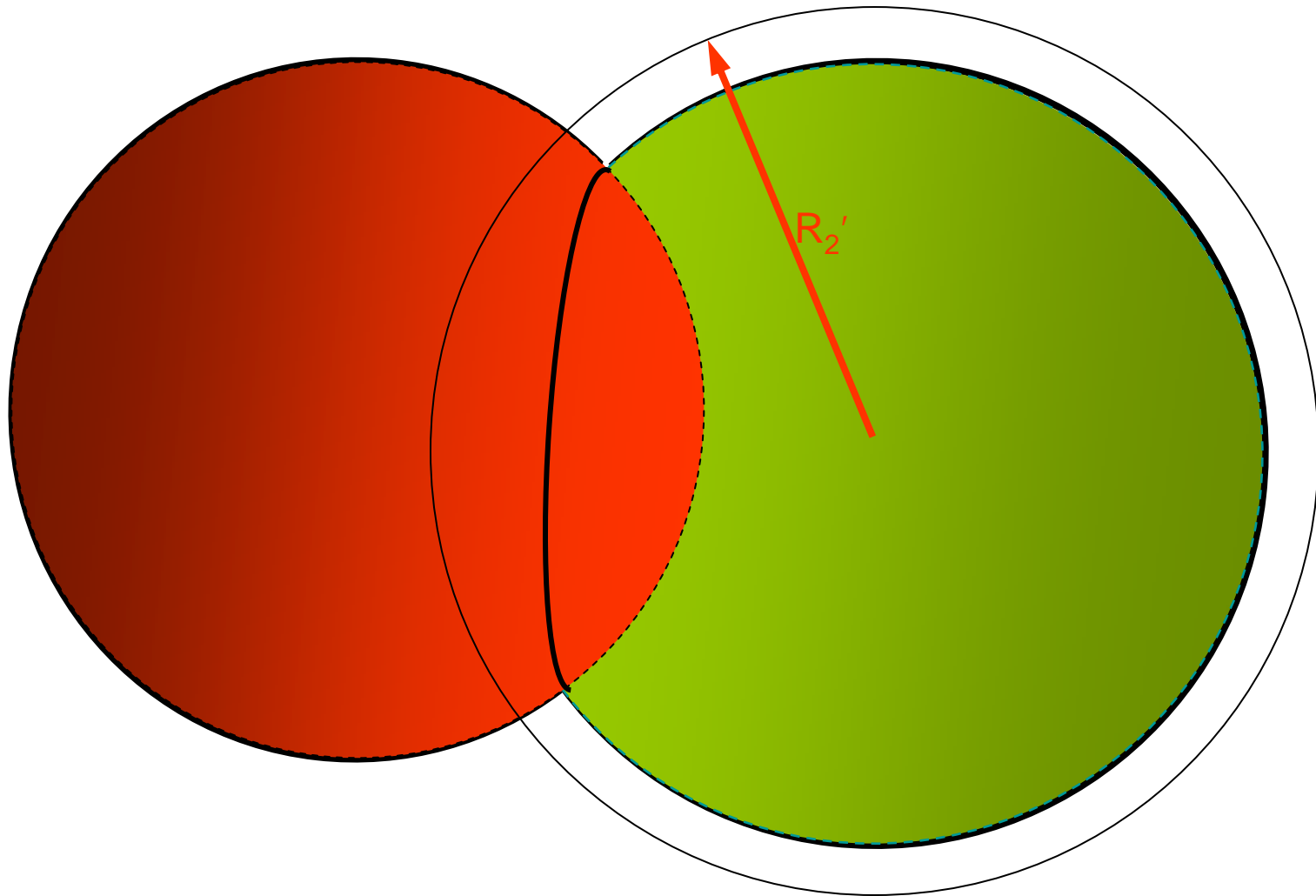


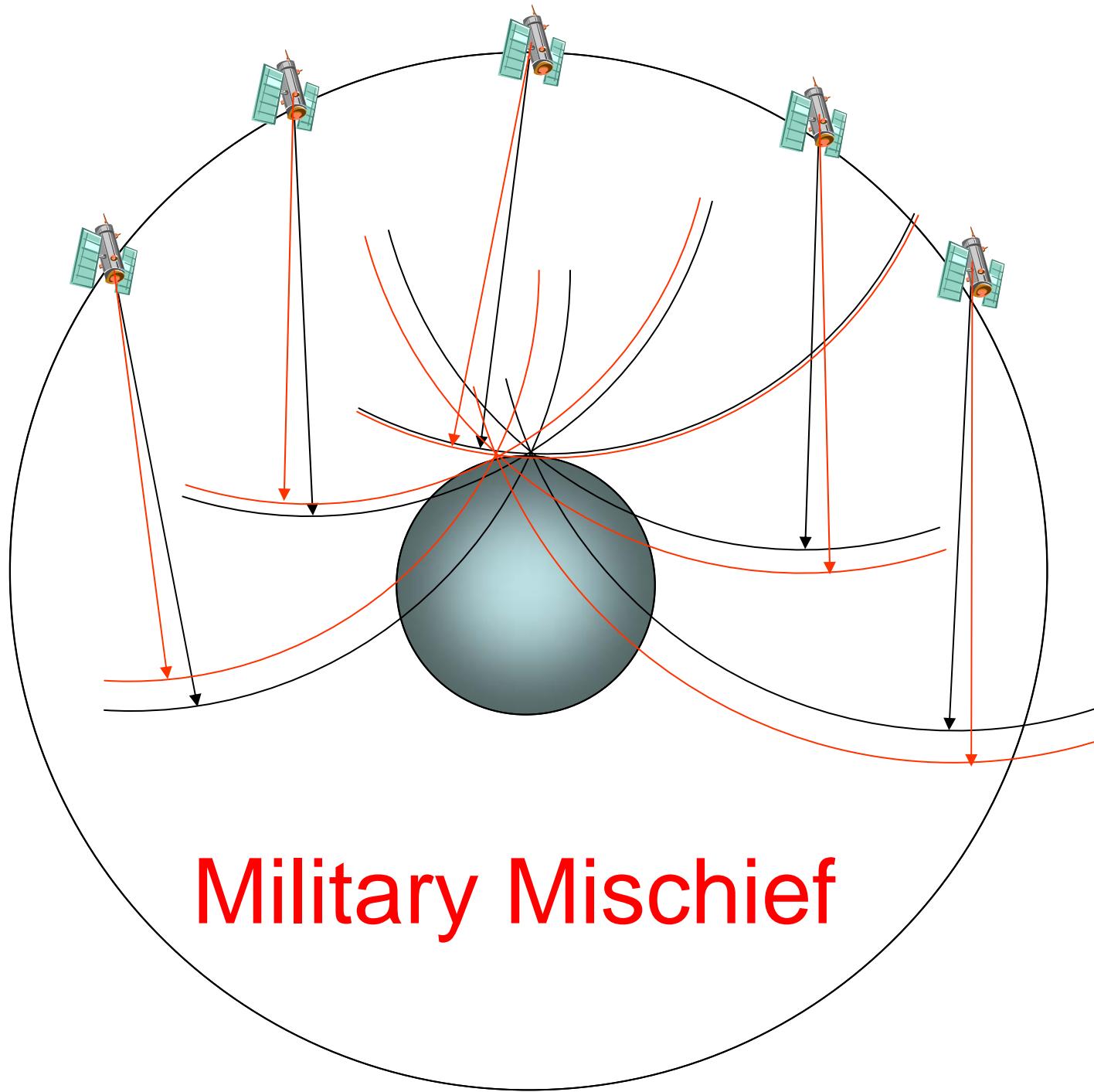


“Fast” Receiver Clock = ahead of correct time

“Slow” Receiver Clock = behind correct time

Selective Availability/Spoofing Intentional Error in Signal

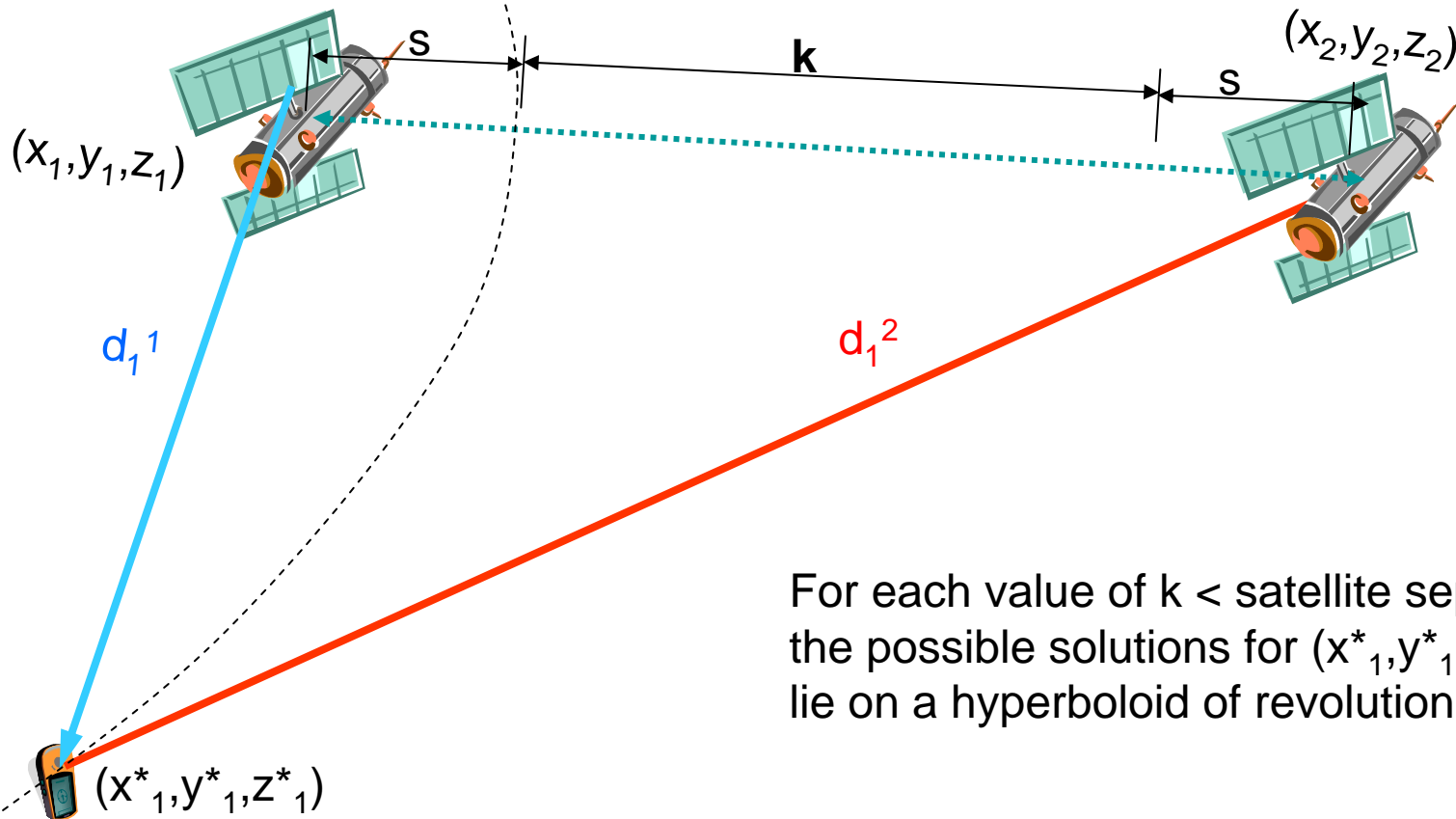




Military Mischief

Differencing:

$$d_1^1 - d_1^2 = k$$

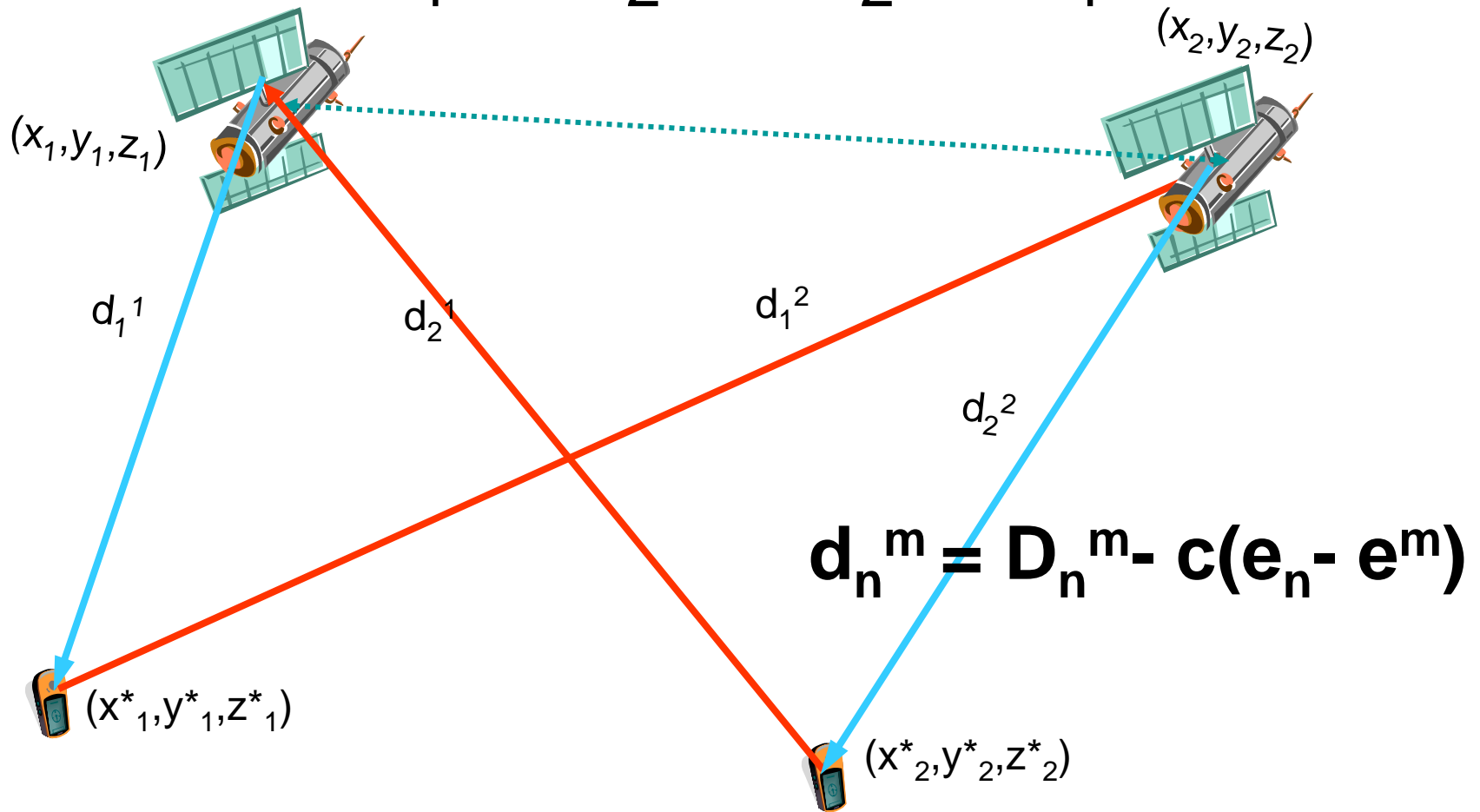


For each value of $k <$ satellite separation,
the possible solutions for (x^*, y^*, z^*)
lie on a hyperboloid of revolution

A clock offset in the receiver does not
have any effect on the measured value of k

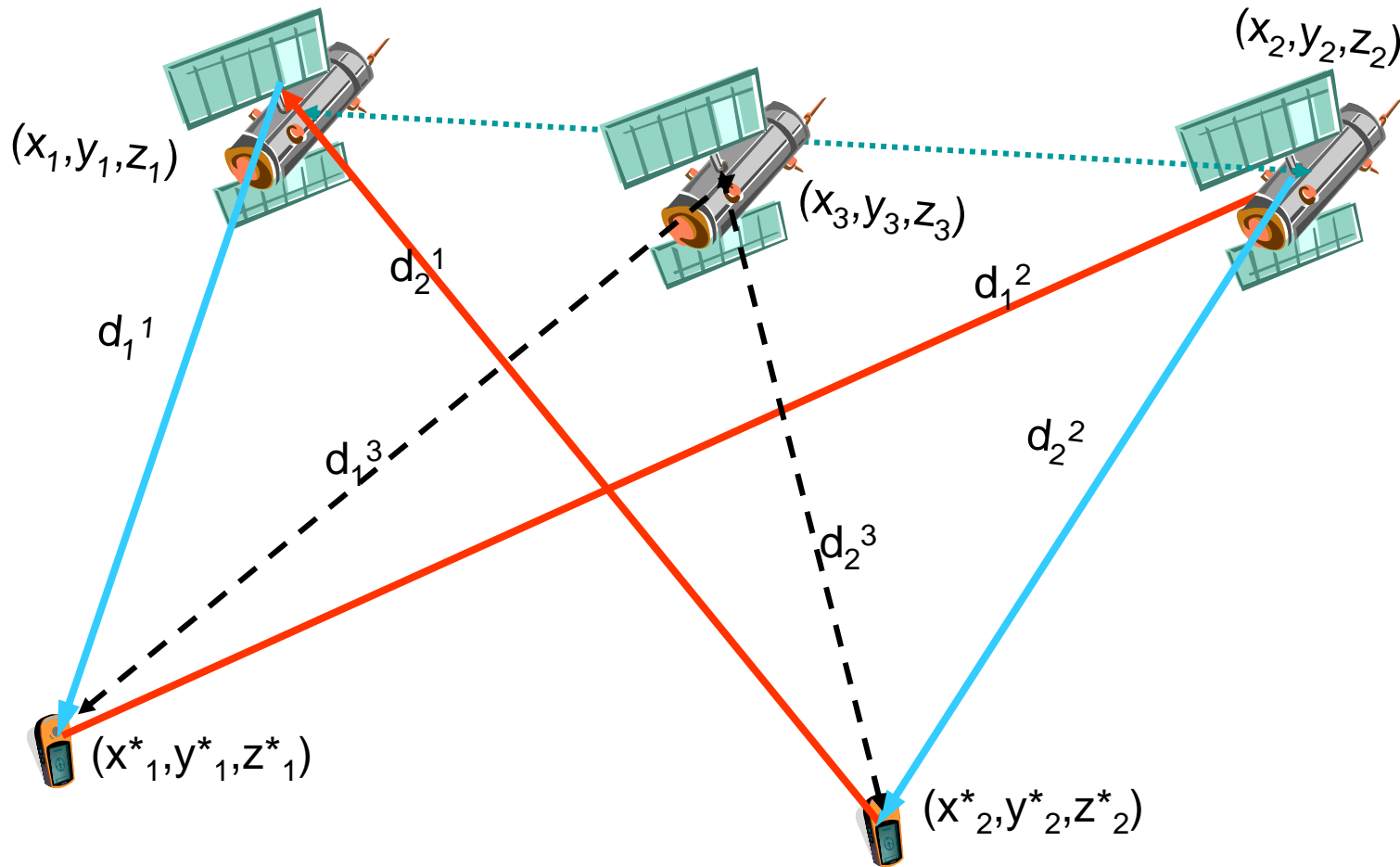
Double Difference:

$$d_1^1 - d_2^1 + d_2^2 - d_1^2$$
$$= D_1^1 - D_2^1 + D_2^2 - D_1^2$$



Not all double differences are independent:

$$(d_1^1 - d_2^1 + d_2^2 - d_1^2) - (d_1^1 - d_1^3 + d_2^3 - d_2^1) \\ = d_2^2 - d_1^2 + d_1^3 - d_2^3$$



Challenge: Find a maximal set of independent double differences

	S ₁	S ₂	S ₃	S ₄	S ₅	S ₆	S ₇	S ₈	S ₉	S ₁₀	S ₁₁	S ₁₂
R ₁	1	1	0	1	0	1	0	1	1	1	1	0
R ₂	0	1	0	1	0	0	1	0	1	0	1	0
R ₃	1	1	0	0	1	1	0	0	0	1	1	0
R ₄	0	0	1	1	1	0	0	0	1	0	0	1
R ₅	1	0	1	1	1	1	0	0	0	1	0	1
R ₆	0	1	0	1	0	0	1	0	1	0	1	0
R ₇	0	0	0	0	0	0	1	1	0	0	0	1
R ₈	1	1	0	0	1	0	0	0	0	1	1	0
R ₉	0	0	0	0	1	0	1	0	1	0	0	0
R ₁₀	1	0	1	0	1	0	0	0	0	1	0	1
R ₁₁	1	1	0	1	0	1	0	1	1	1	1	0
R ₁₂	0	1	0	1	0	0	1	0	1	0	1	0
R ₁₃	1	1	0	0	1	1	0	0	0	1	1	0
R ₁₄	0	0	1	1	1	0	0	0	1	0	0	1
R ₁₅	1	0	1	1	1	1	1	0	0	1	0	1

Challenge: Find a maximal set of independent double differences

	S ₁	S ₂	S ₃	S ₄	S ₅	S ₆	S ₇	S ₈	S ₉	S ₁₀	S ₁₁	S ₁₂
R ₁	1	1	0	1	0	1	0	1	1	1	1	0
R ₂	0	1	0	1	0	0	1	0	1	0	1	0
R ₃	1	1	0	0	1	1	0	0	0	1	1	0
R ₄	0	0	1	1	1	0	0	0	1	0	0	1
R ₅	1	0	1	1	1	1	0	0	0	1	0	1
R ₆	0	1	0	1	0	0	1	0	1	0	1	0
R ₇	0	0	0	0	0	0	1	1	0	0	0	1
R ₈	1	1	0	0	1	0	0	0	0	1	1	0
R ₉	0	0	0	0	1	0	1	0	1	0	0	0
R ₁₀	1	0	1	0	1	0	0	0	0	1	0	1
R ₁₁	1	1	0	1	0	1	0	1	1	1	1	0
R ₁₂	0	1	0	1	0	0	1	0	1	0	1	0
R ₁₃	1	1	0	0	1	1	0	0	0	1	1	0
R ₁₄	0	0	1	1	1	0	0	0	1	0	0	1
R ₁₅	1	0	1	1	1	1	1	0	0	1	0	1

Response counts and sensitive data

50	11	9	15	15
10	1	0	5	4
15	3	4	4	4
5	3	0	0	2
20	4	5	6	5

5650	1500	850	1500	1800
1300	300	0	500	500
1900	400	500	600	400
950	550	0	0	400
1500	250	350	400	500

- Additive tables showing (left) the number of respondents and (right) their cumulative totals
- The challenge: want to provide as much useful information as possible without **disclosing** data from cells that come from only 1 or 2 respondents

The adversary knows arithmetic

- Blanking out the sensitive cells is not sufficient to prevent disclosure
- Blanking out some well-chosen additional cells will provide some protection of confidential data

5650	1500	850	1500	1800
1300	***	0	500	500
1900	400	500	600	400
950	550	0	0	***
1500	250	350	400	500

5650	1500	850	1500	1800
1300	***	0	500	***
1900	400	500	600	400
950	***	0	0	***
1500	250	350	400	500

Additive Arrays Form a Subspace

- The subspace of additive arrays is closed under addition, subtraction, and scaling.
- The set of additive tables is closed under addition, but not under subtraction.
- The difference of two additive tables is not necessarily a table, but it is always an additive array.
- *Adjustments* to additive arrays that return additive arrays must themselves be additive arrays.

14	7	7
8	5	3
6	2	4

-

14	7	7
8	1	7
6	6	0

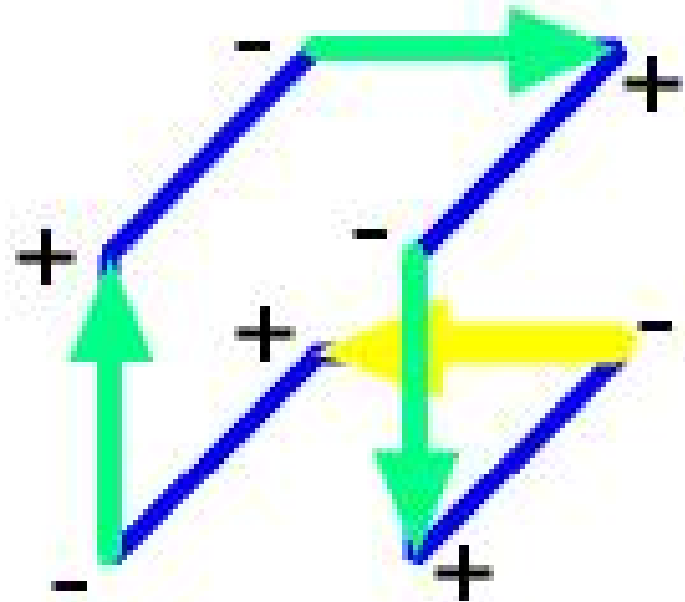
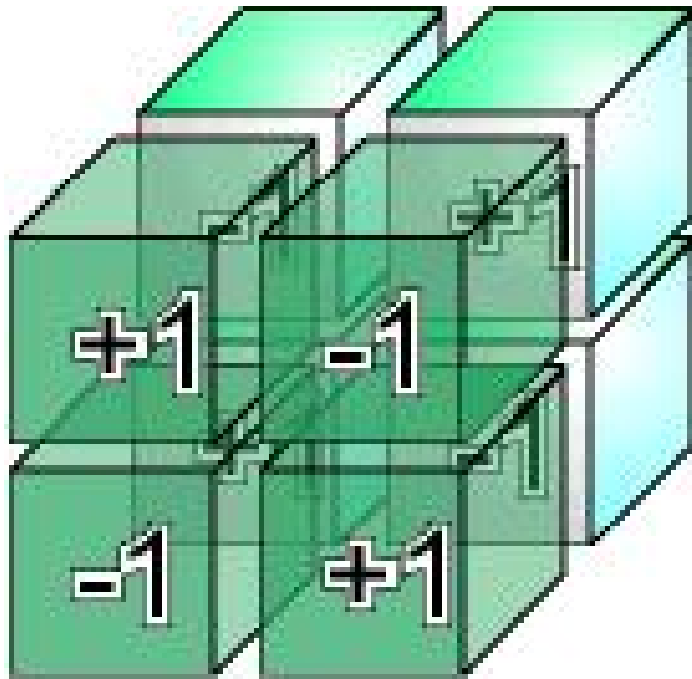
0	0	0
0	4	-4
0	-4	4

Additive Array Space Generators

$\mathbf{e}_{m_1 m_2} =$

	Col 0	Col 1	...	Col m_2	...	Col i_2
Row 0	1	0	:	1	..	0
Row 1	0	0	:	0	..	0
:	0	0	...	0
Row m_1	1	0	0	1	0	0
:	:	:	:	0	0	0
Row i_1	0	0	0	0	0	0

Plus-minus paths in 3-D



Cell-wise Rounding

4.8	1.2	1.2	1.2	1.2
1.6	0.4	0.4	0.4	0.4
1.6	0.4	0.4	0.4	0.4
1.6	0.4	0.4	0.4	0.4

Controlled Rounding

5	1	1	1	1
2	0	0	0	0
2	0	0	0	0
2	0	0	0	0

5	1	1	1	2
2	1	0	0	1
2	0	1	0	1
1	0	0	1	0

More to do—students welcome

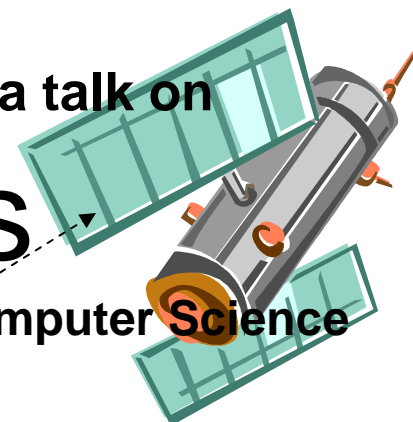
- What about 3-way (3D) tables?
- What about “linked” sets of tables?
- What about enforcing rules for protecting ranges instead of values?
- What about using dual-space/dimension theory...



The OSU Radical Pi Math Club invites you to a talk on

Plus-Minus Paths

by Alan Saalfeld, Professor of Geodetic Science and Computer Science



Abstract: Learn how a GPS receiver works. Learn what mathematics made it work even better than the military wanted it to! Learn more about that mathematics and its applications in the seemingly contradictory areas of (1) improving accuracy of GPS measurements and (2) adding ambiguity and uncertainty to tabular Census data (with the aim of protecting respondent confidentiality).



Wednesday February 22 at 5:00 pm in MW 724

Free pizza and pop