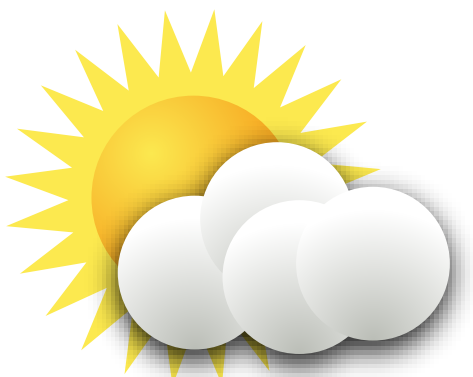
Beware of Optimistic Weather Forecasts

C. Boura, A. Canteaut, and C. De Cannière



August 17, 2010

Wednesday, August 18, 2010

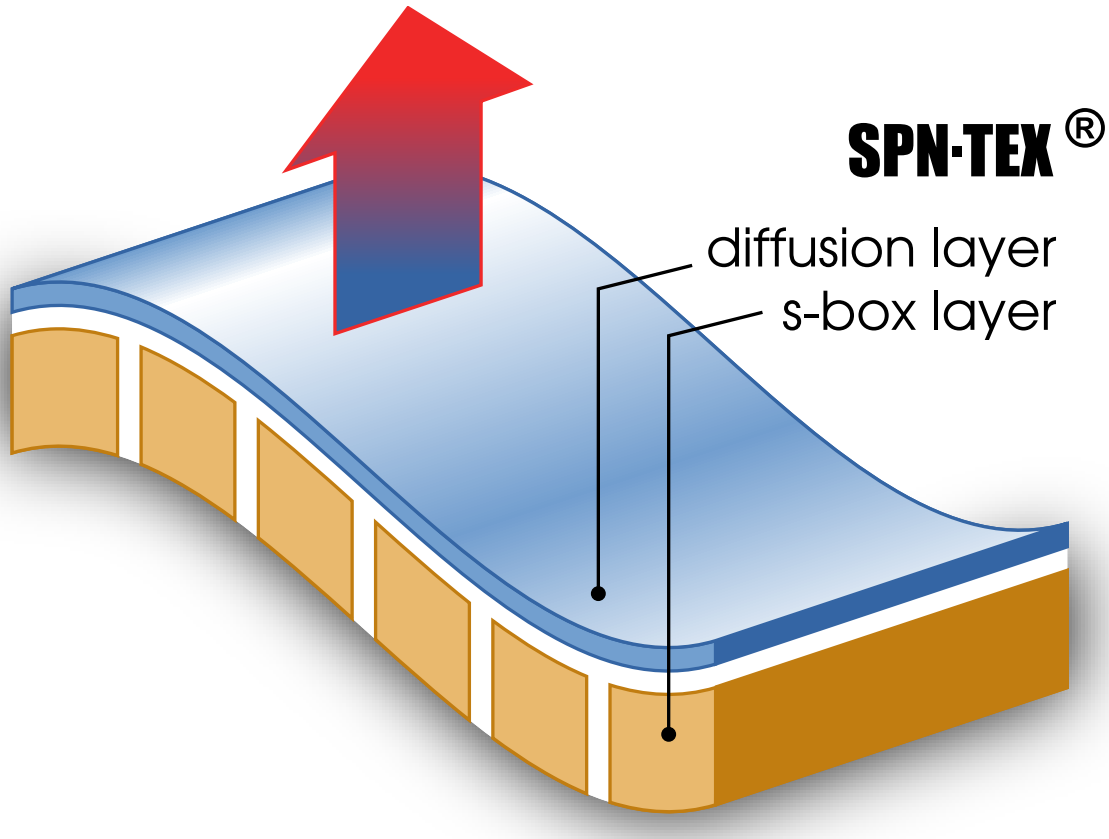
18:00 – 20:00: **Beach Barbecue at Goleta Beach**

One Fundamental Question

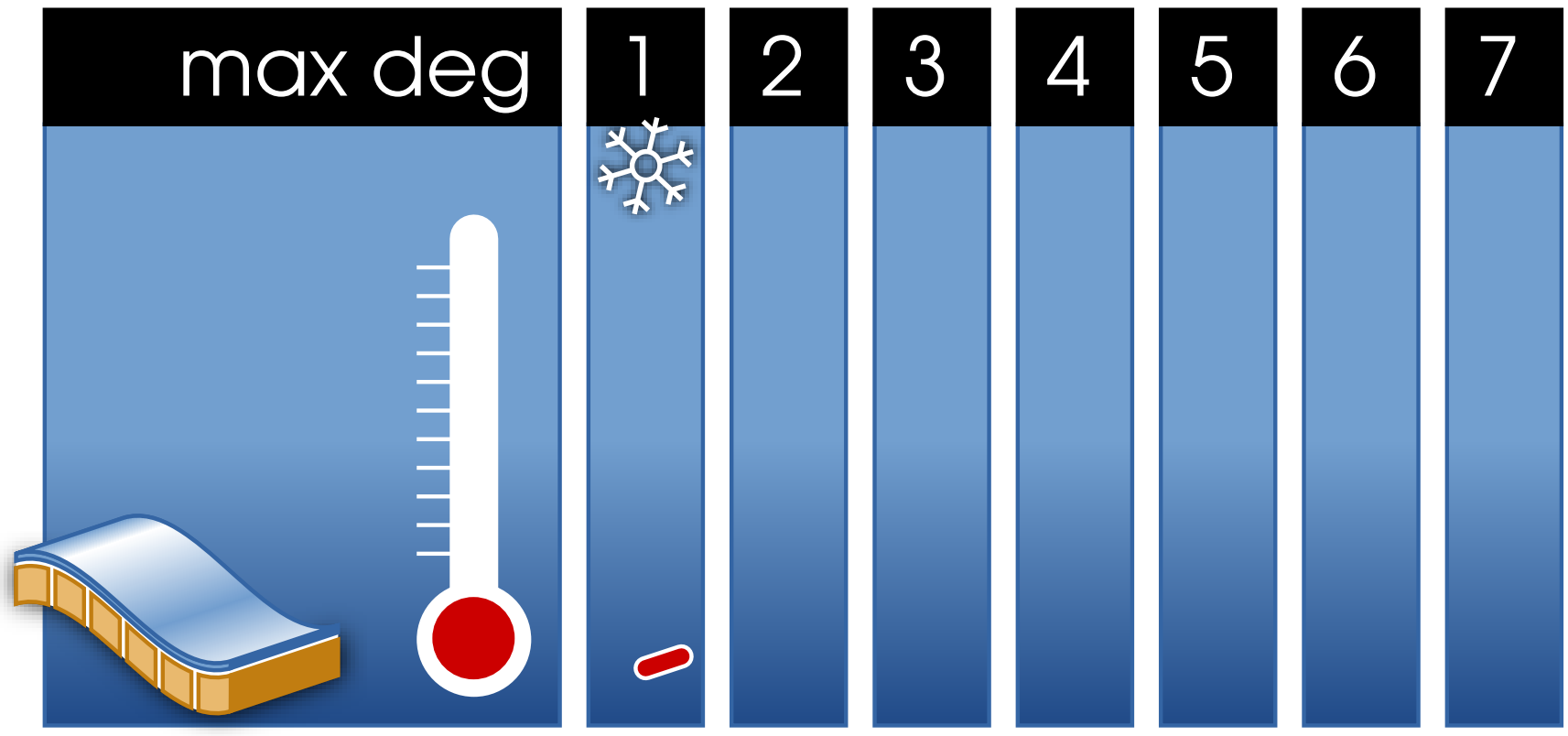
Q: What to wear?

SPN Fabric

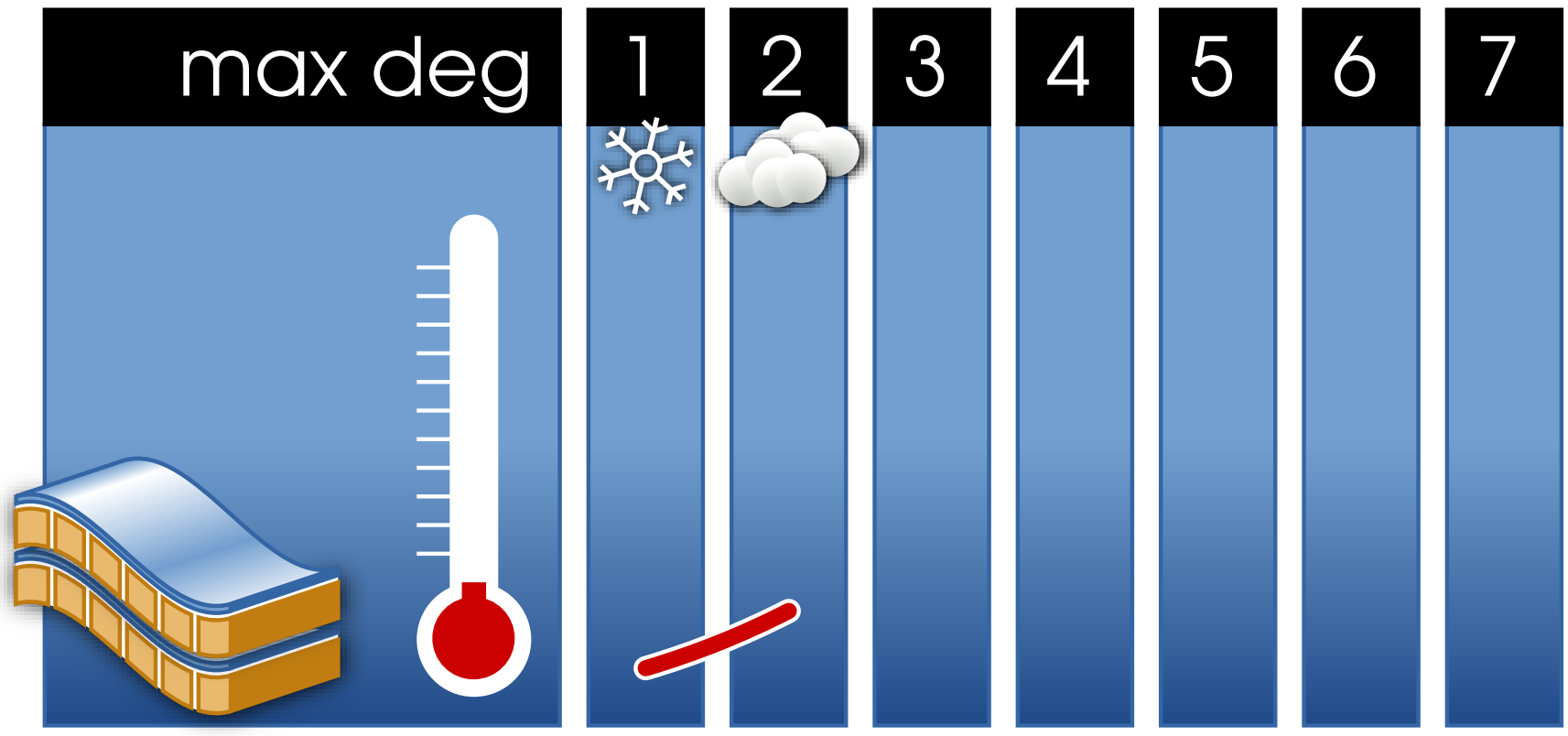
A: High-Tech Clothing



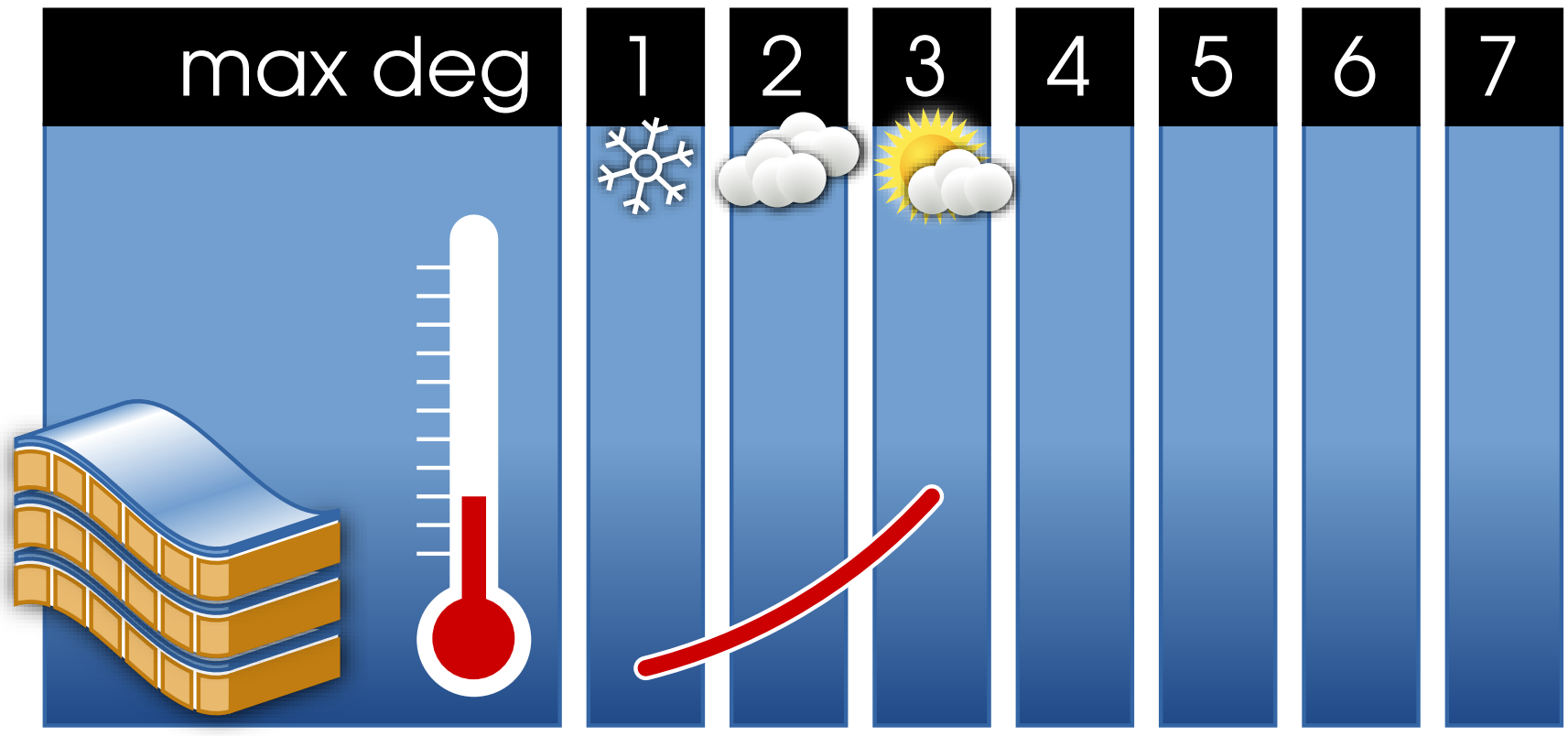
Maximum Degree (Old Bound)



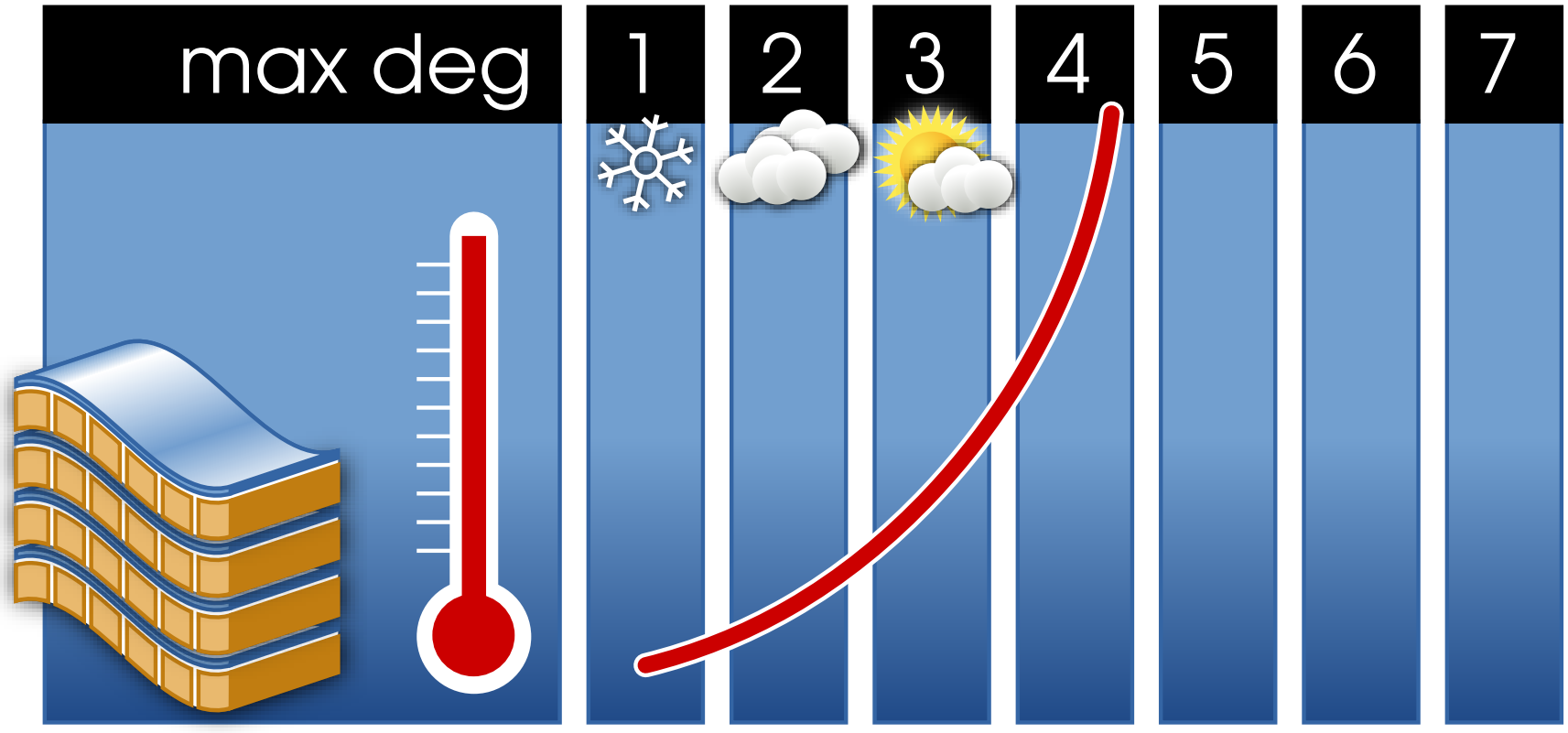
Maximum Degree (Old Bound)



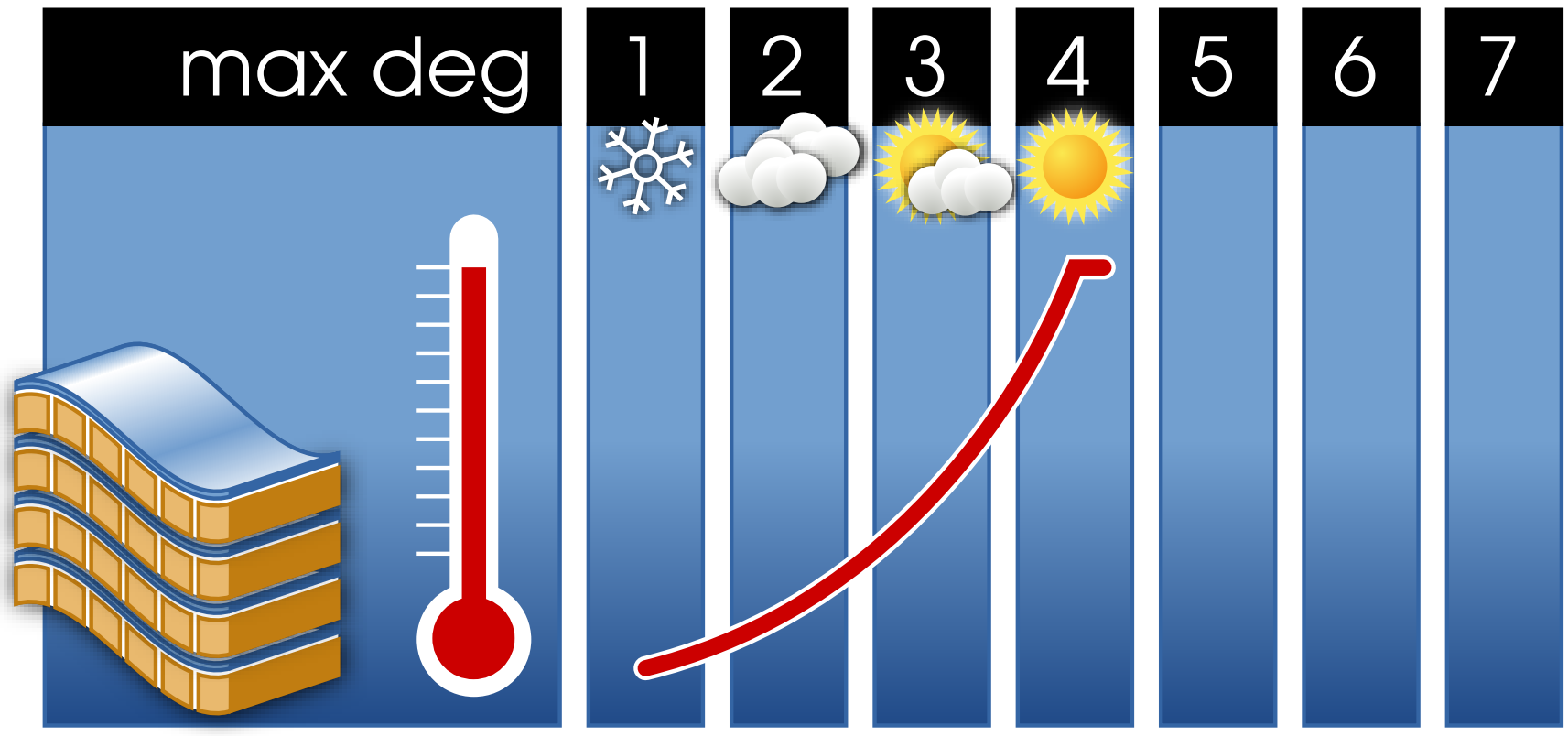
Maximum Degree (Old Bound)



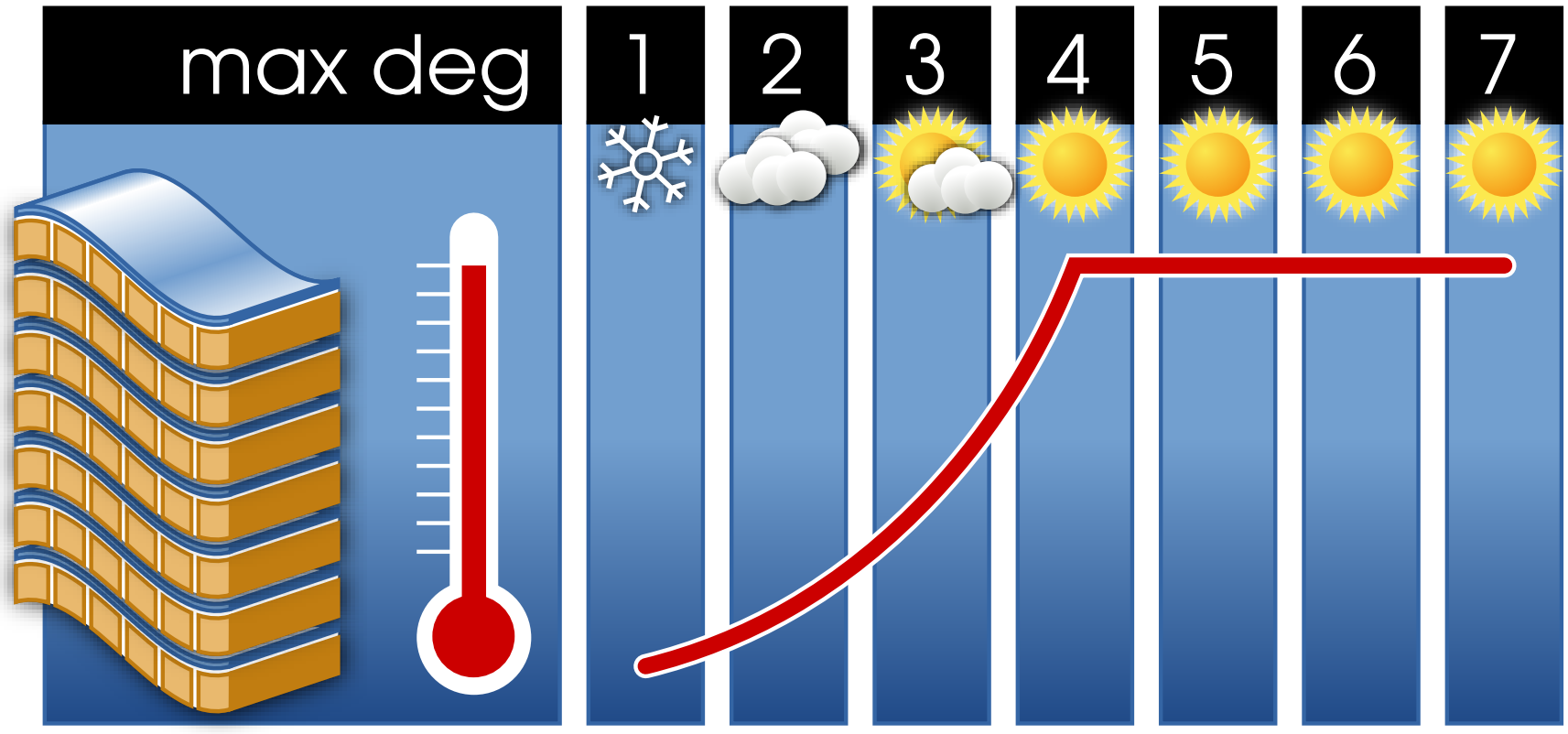
Maximum Degree (Old Bound)



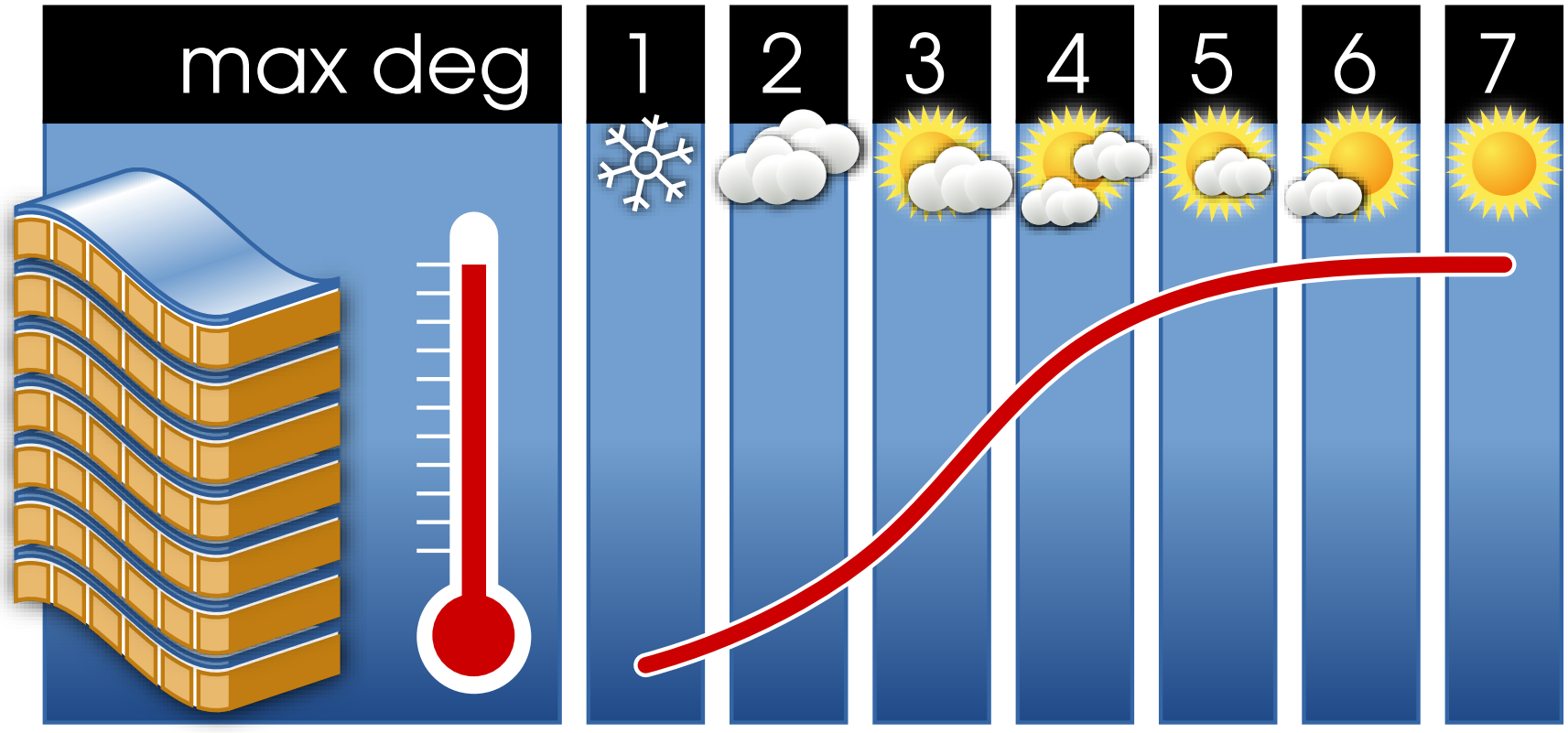
Maximum Degree (Old Bound)



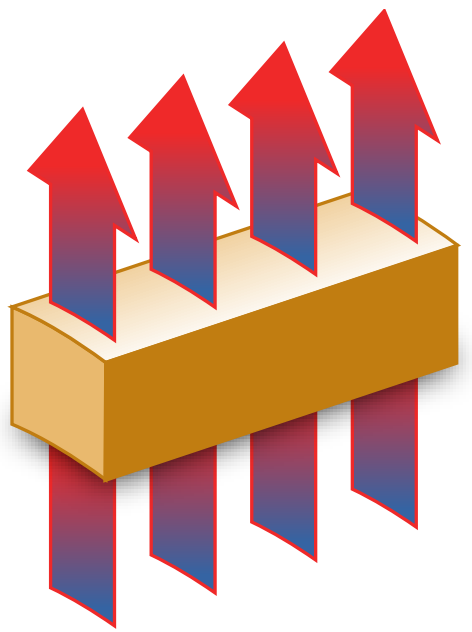
Maximum Degree (Old Bound)



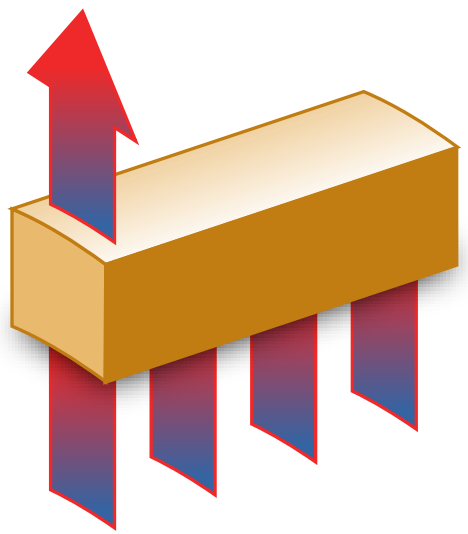
Maximum Degree (New Bound)



Why Does the Growth Slow Down?



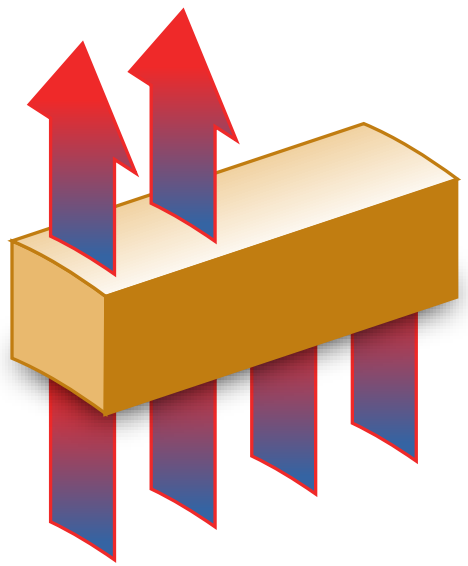
Why Does the Growth Slow Down?



- **Definition of δ_i:**
  maximum degree of any product of i output bits.

i	δ_i
1	

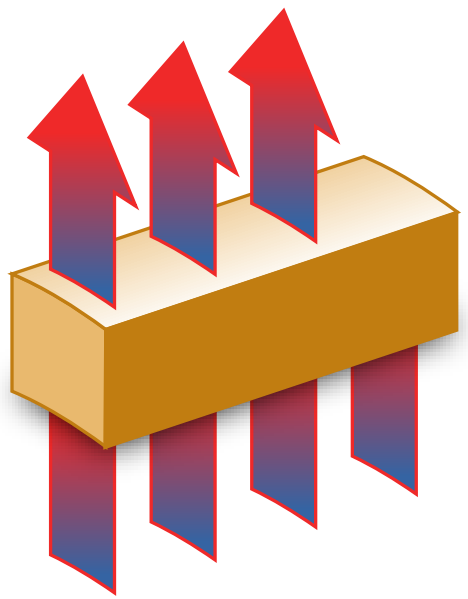
Why Does the Growth Slow Down?



- **Definition of δ_i:** maximum degree of any product of i output bits.

i	δ_i
1	3
2	

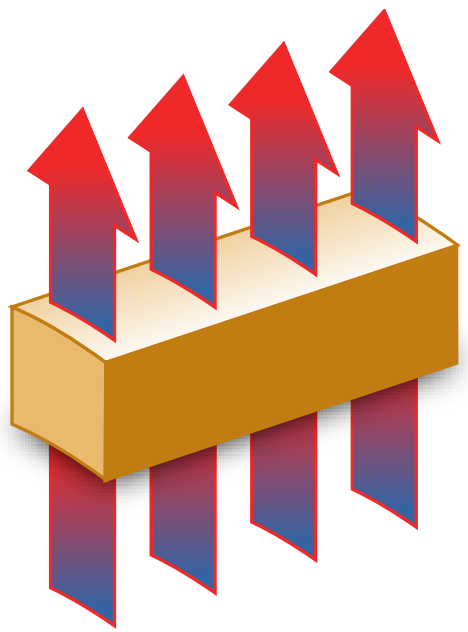
Why Does the Growth Slow Down?



- **Definition of δ_i:** maximum degree of any product of i output bits.

i	δ_i
1	3
2	3
3	

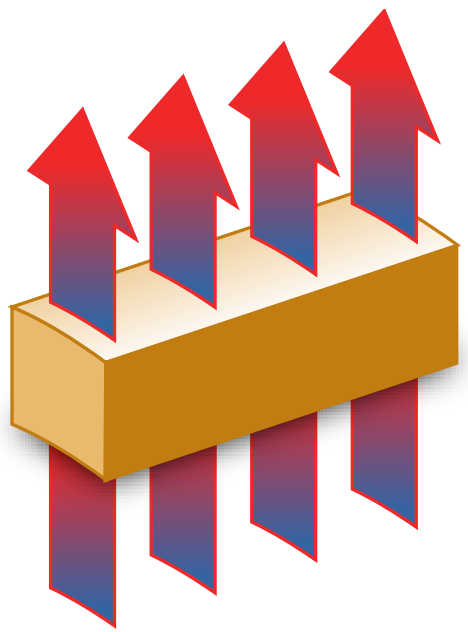
Why Does the Growth Slow Down?



- **Definition of δ_i:** maximum degree of any product of i output bits.

i	δ_i
1	3
2	3
3	3
4	

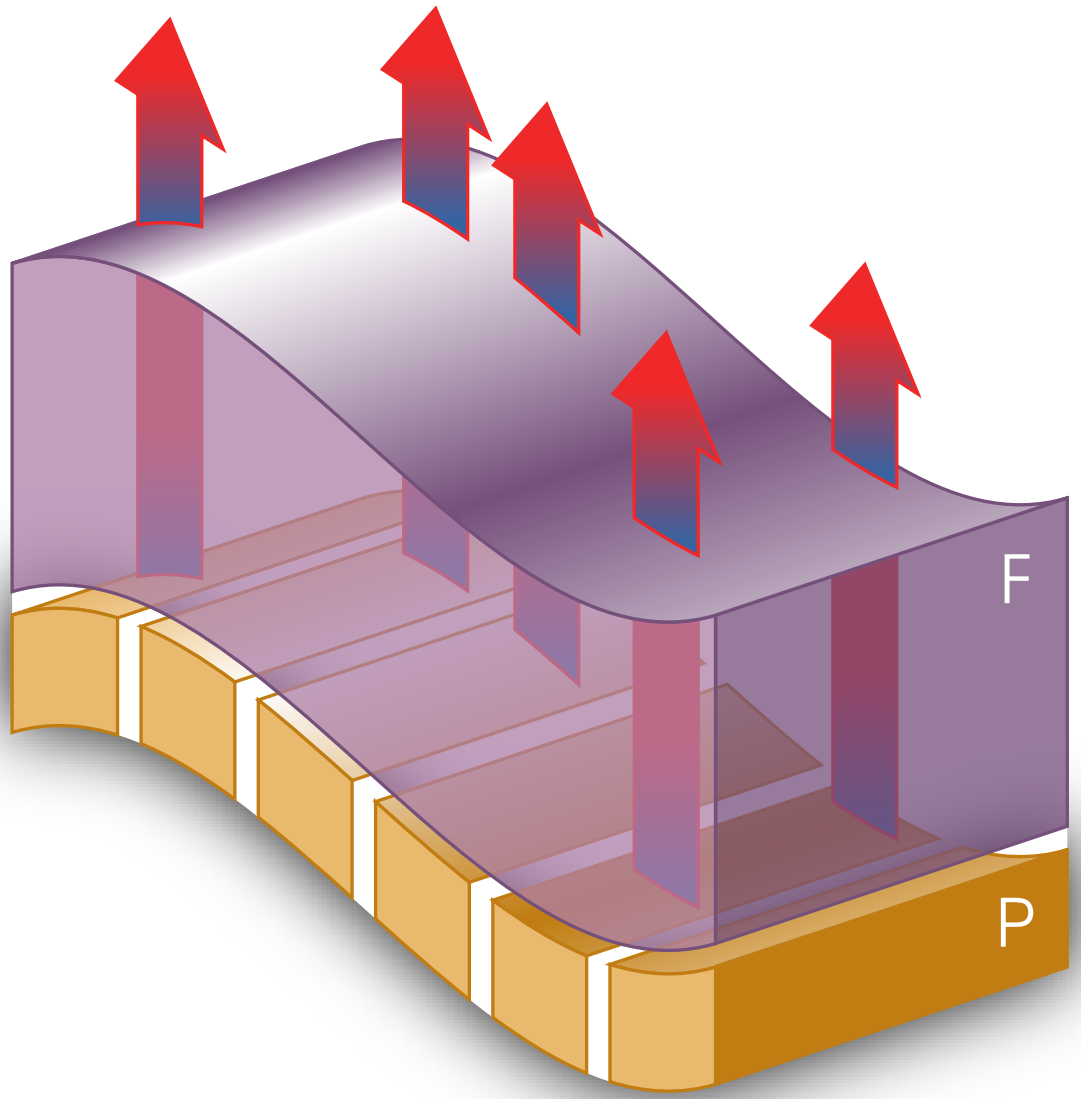
Why Does the Growth Slow Down?



- **Definition of δ_i:** maximum degree of any product of i output bits.

i	δ_i
1	3
2	3
3	3
4	4

Why Does the Growth Slow Down?



The New Bound

Theorem

$$\frac{n - \deg(F)}{n - \deg(F \circ P)} \leq \max_{0<i<n_0} \frac{n_0 - i}{n_0 - \delta_i}.$$

Applications

- **Keccak:** Zero-sum partition for full permutation.
- **Luffa v1:** Higher-order differential for short messages.