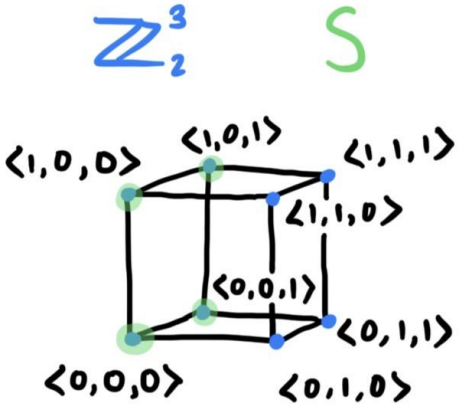
What's a vector subspace?

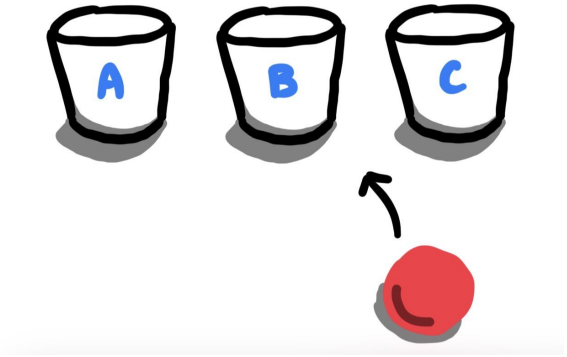
Vector subspaces are smaller groups of vectors within a given vector space. They're defined by **basis vectors**, and the vectors in the subspace consist of all possible combinations of the **basis vectors**.

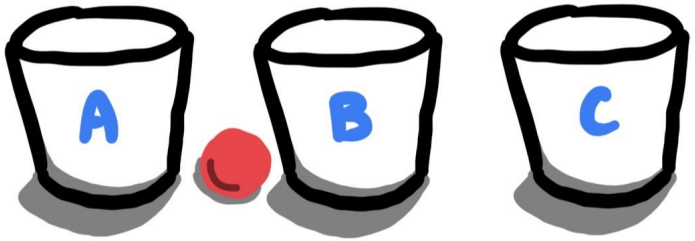


$$S = \{a\langle 1,0,0\rangle + b\langle 0,0,1\rangle, \text{ where } a,b \in \mathbb{Z}_2\}$$

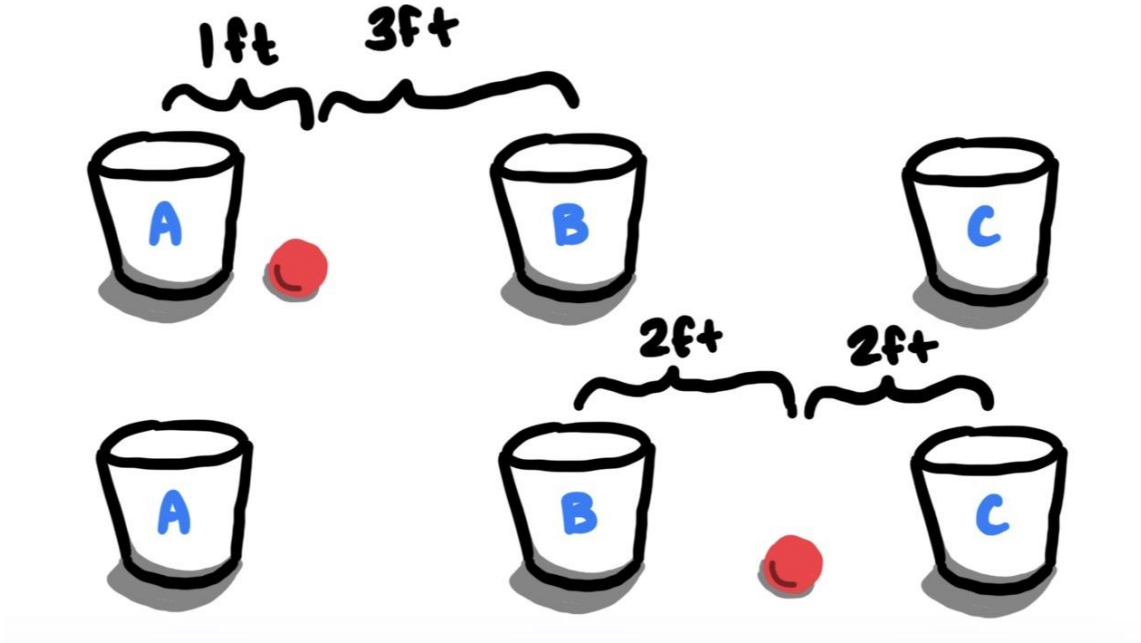
This translates roughly to: "The subspace **S** contains all possible sums of the basis vectors a<1, 0, 0>+b<0, 0, 1>, where a and b are in base-2."

Hamming distance



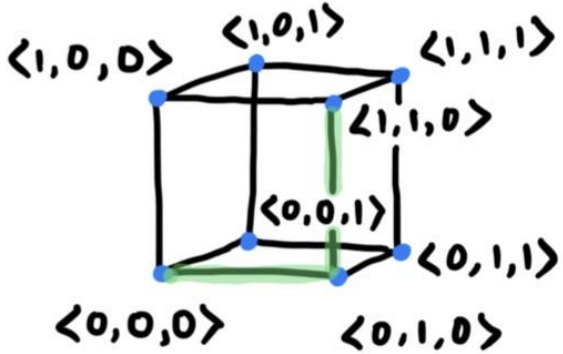


Hamming distance



Hamming distance

The **Hamming distance** between two vectors is the number of bits that differ between them. The **minimum Hamming distance** for a vector space or subspace is the smallest Hamming distance between two vectors in the space / subspace.



$\mathbb{Z}_2^3$

hamming distance between <0,0,0> and <1,1,0> is 2.

the minimum hamming distance for this space is 1 (look at <0,0,0> and <0,0,1>, for example)

(note: for any vector space $\mathbb{Z}_2^n$, its maximum Hamming distance is n. Can you explain why?)

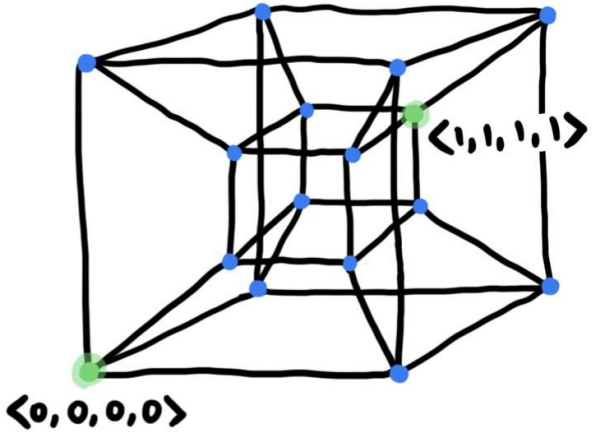
Hamming codes

- we want to define a Hamming space that's **sparse** - that means, the **minimum Hamming distance** of the space is as large as possible (just like with the balls + bins analogy, we want to "place" them very far apart)
- the number of errors that can be detected and corrected by a Hamming code depends on the **minimum Hamming distance** of the space you use
- spaces that can detect if there are up to k errors are called **k-error detecting spaces**, and ones that can correct up to n errors are called **n-error correcting** spaces

Error correction with Hamming codes

$S = \{\langle 0,0,0,0\rangle, \langle 1,1,1,1\rangle\}$

minimum Hamming distance = 4



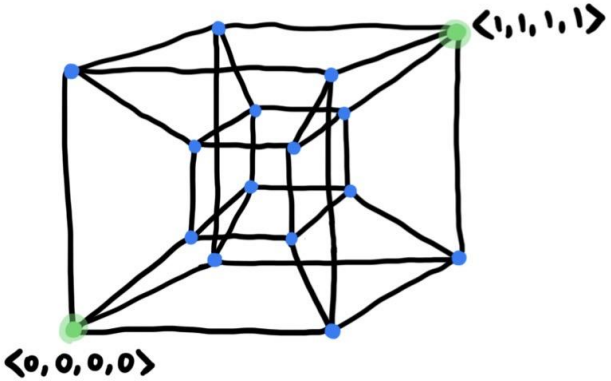
we can detect that there has been an error if there are <4 errors.
however, we can only correct 1 error accurately.

so, S is 3-error detecting and 1-error correcting

Error correction with Hamming codes

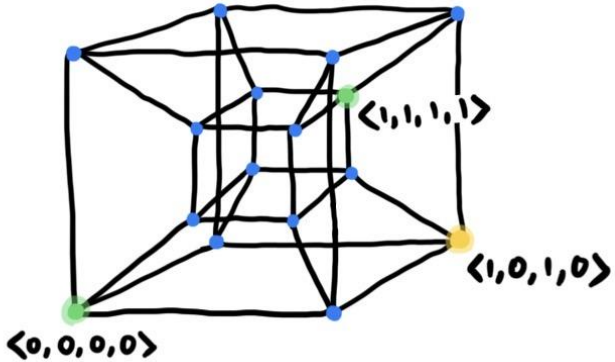
$S = \{\langle 0,0,0,0\rangle, \langle 1,1,1,1\rangle\}$

minimum Hamming distance = 4



say we recieve the transmission ⟨1,0,1,0⟩.

we know there's been at least one error—
but because ⟨1,0,1,0⟩ is the same distance from both ⟨0,0,0,0⟩ and ⟨1,1,1,1⟩, we don't know how to correct it.



Error correction with Hamming codes

in general, a Hamming space with minimum Hamming distance d

- can detect that there has been an error, if there are up to $d-1$ errors
- can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors

(this means "rounded down")