So the Gnosis PM contracts 2.x contains better support for conditional markets.

Some details are here but to summarize, for two questions with outcomes [A, B, C] and [HI, LO], conditional markets can be made:

Wherein the predictive assets can be redeemed in any order of its constituent conditions:

This is done with a mapping from account => position id => balance, where a position id is a hash(collateralERC20Address . truncated32ByteSum({hash(condition id . index set) : outcome collection})).

I'm wondering how safe using a truncated32ByteSum of hashes to represent a set of objects as a key for a mapping is. In this case, this is further wrapped inside of another hash due to the use case. Maybe somebody can point me to similar uses of this idea?

Also, unions of outcomes are represented by bit arrays which are called index sets

. I wanted to fully generalize Boolean formulas as keys in an mapping, but that doesn't seem to be possible, meaning (A&HI)|(B&LO) can't be represented as a single key whereas (A&HI)|(B&HI) = (A|B)&HI can.