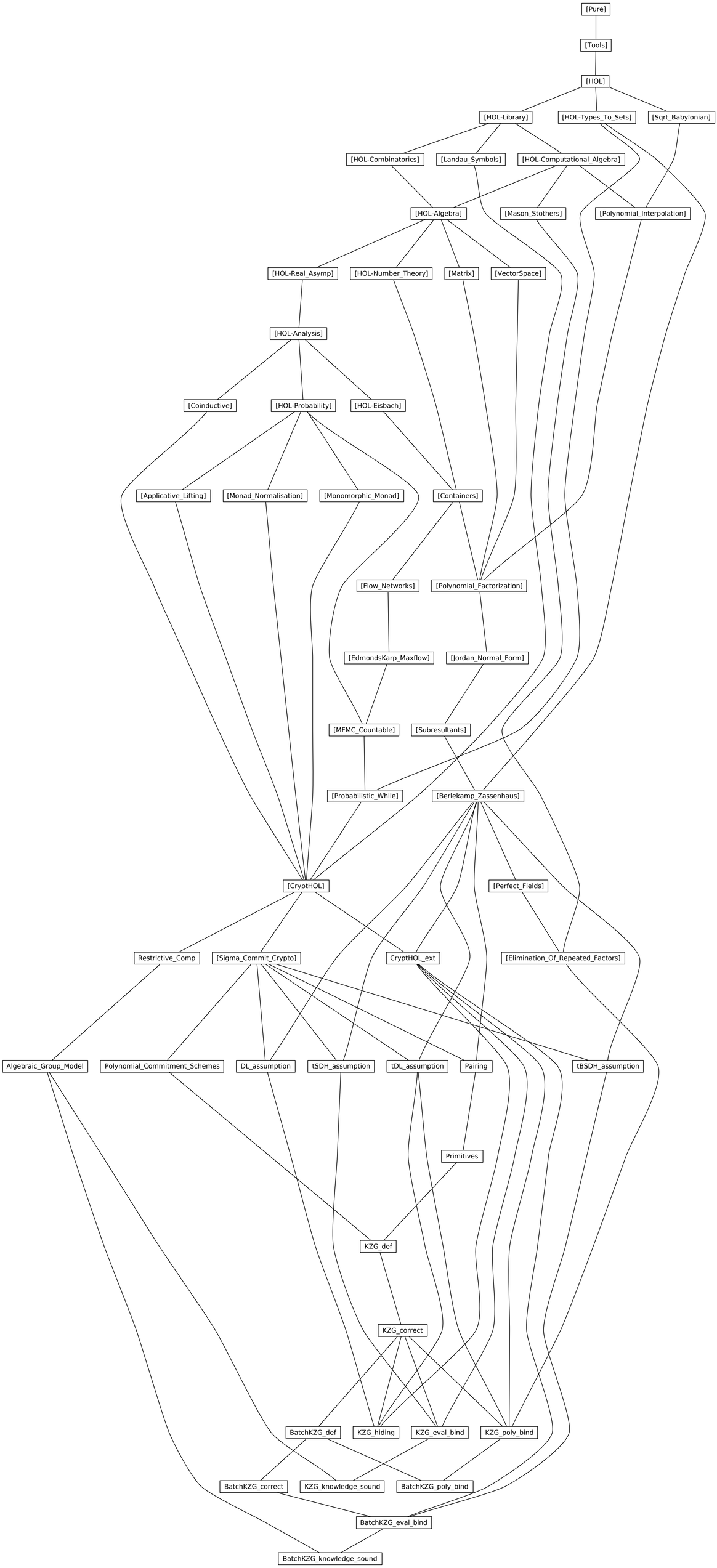
[Pure]
[Tools]
[HOL]
[HOL-Library]
[HOL-Types_To_Sets]
[Sqrt_Babylonian]
[HOL-Combinatorics]
[Landau_Symbols]
[HOL-Computational_Algebra]
[HOL-Algebra]
[Mason_Stothers]
[Polynomial_Interpolation]
[HOL-Real_Asymp]
[HOL-Number_Theory]
[Matrix]
[VectorSpace]
[HOL-Analysis]
[Coinductive]
[HOL-Probability]
[HOL-Eisbach]
[Applicative_Lifting]
[Monad_Normalisation]
[Monomorphic_Monad]
[Containers]
[Flow_Networks]
[Polynomial_Factorization]
[EdmondsKarp_Maxflow]
[Jordan_Normal_Form]
[MFMC_Countable]
[Subresultants]
[Probabilistic_While]
[Berlekamp_Zassenhaus]
[CryptHOL]
[Perfect_Fields]
Restrictive_Comp
[Sigma_Commit_Crypto]
CryptHOL_ext
[Elimination_Of_Repeated_Factors]
Algebraic_Group_Model
Polynomial_Commitment_Schemes
DL_assumption
tSDH_assumption
tDL_assumption
Pairing
tBSDH_assumption
Primitives
KZG_def
KZG_correct
BatchKZG_def
KZG_hiding
KZG_eval_bind
KZG_poly_bind
BatchKZG_correct
KZG_knowledge_sound
BatchKZG_poly_bind
BatchKZG_eval_bind
BatchKZG_knowledge_sound