

# Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers – Scheduling

Jean-Luc Beuchat<sup>1</sup>, Jérémie Detrey<sup>2</sup>, Nicolas Estibals<sup>3</sup>,  
Eiji Okamoto<sup>1</sup>, and Francisco Rodríguez-Henríquez<sup>4</sup>

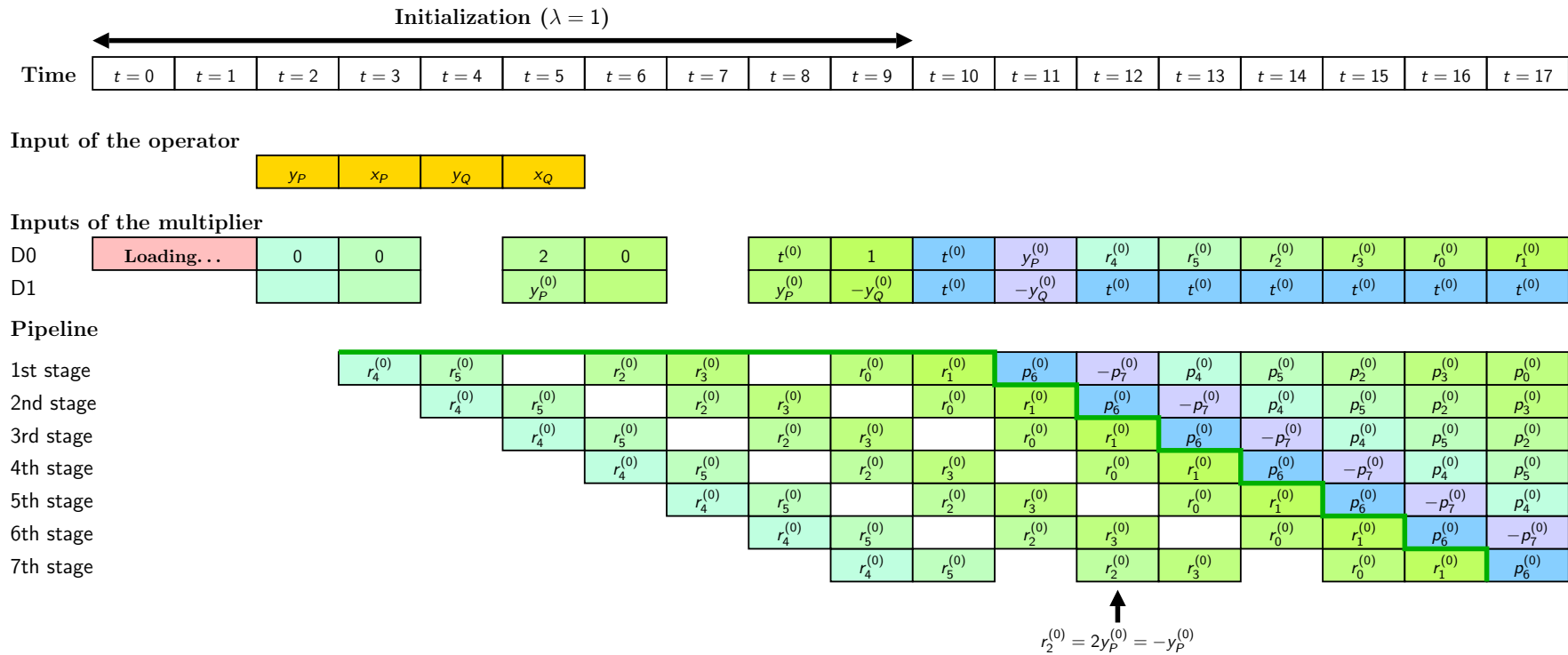
<sup>1</sup> Graduate School of Systems and Information Engineering,  
University of Tsukuba, Tsukuba, Japan

<sup>2</sup> CACAO project-team, INRIA Nancy - Grand Est, Nancy, France

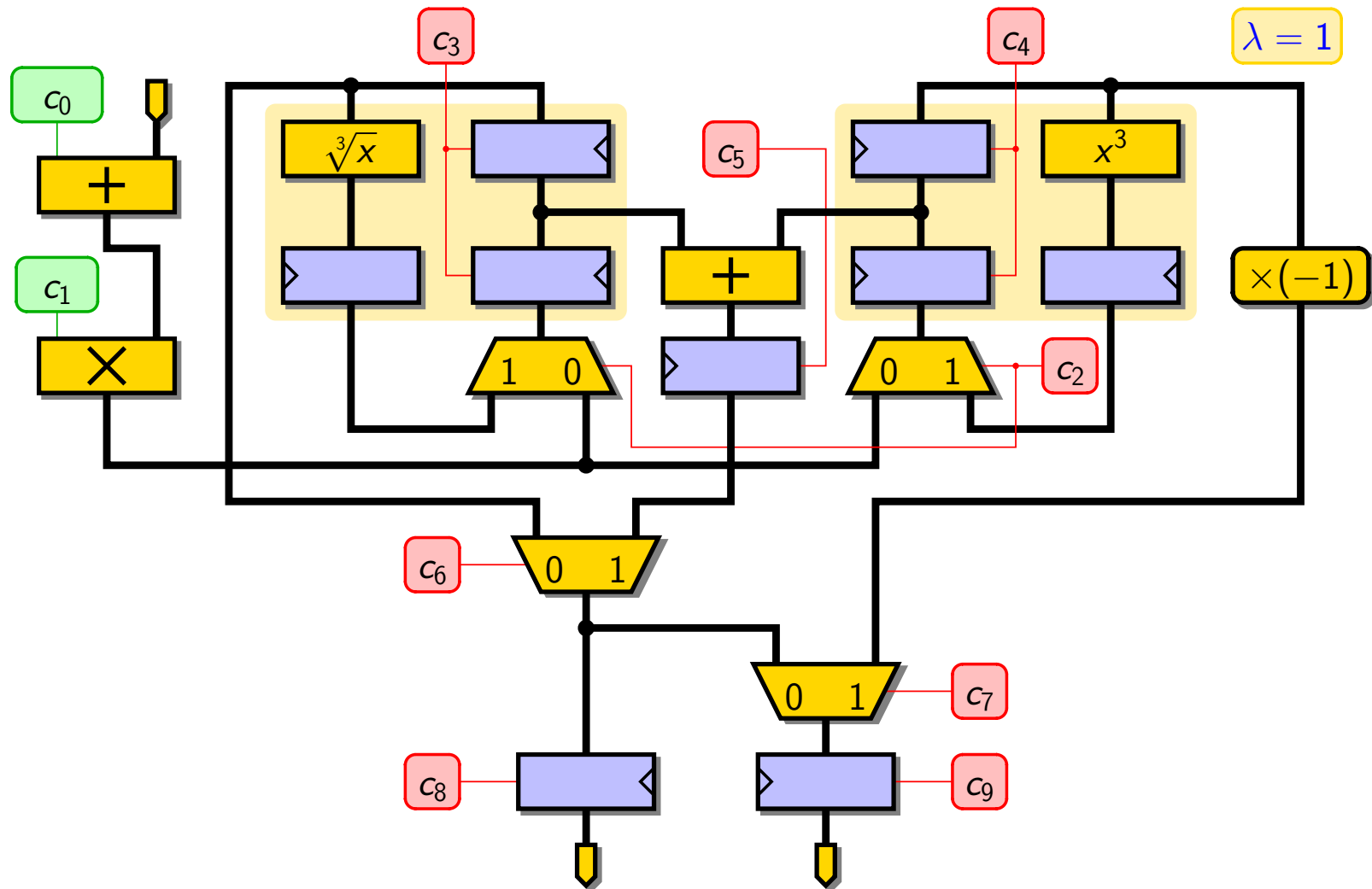
<sup>3</sup> École Normale Supérieure de Lyon, Lyon, France

<sup>4</sup> Computer Science Department,  
Centro de Investigación y de Estudios Avanzados del IPN,  
México City, México

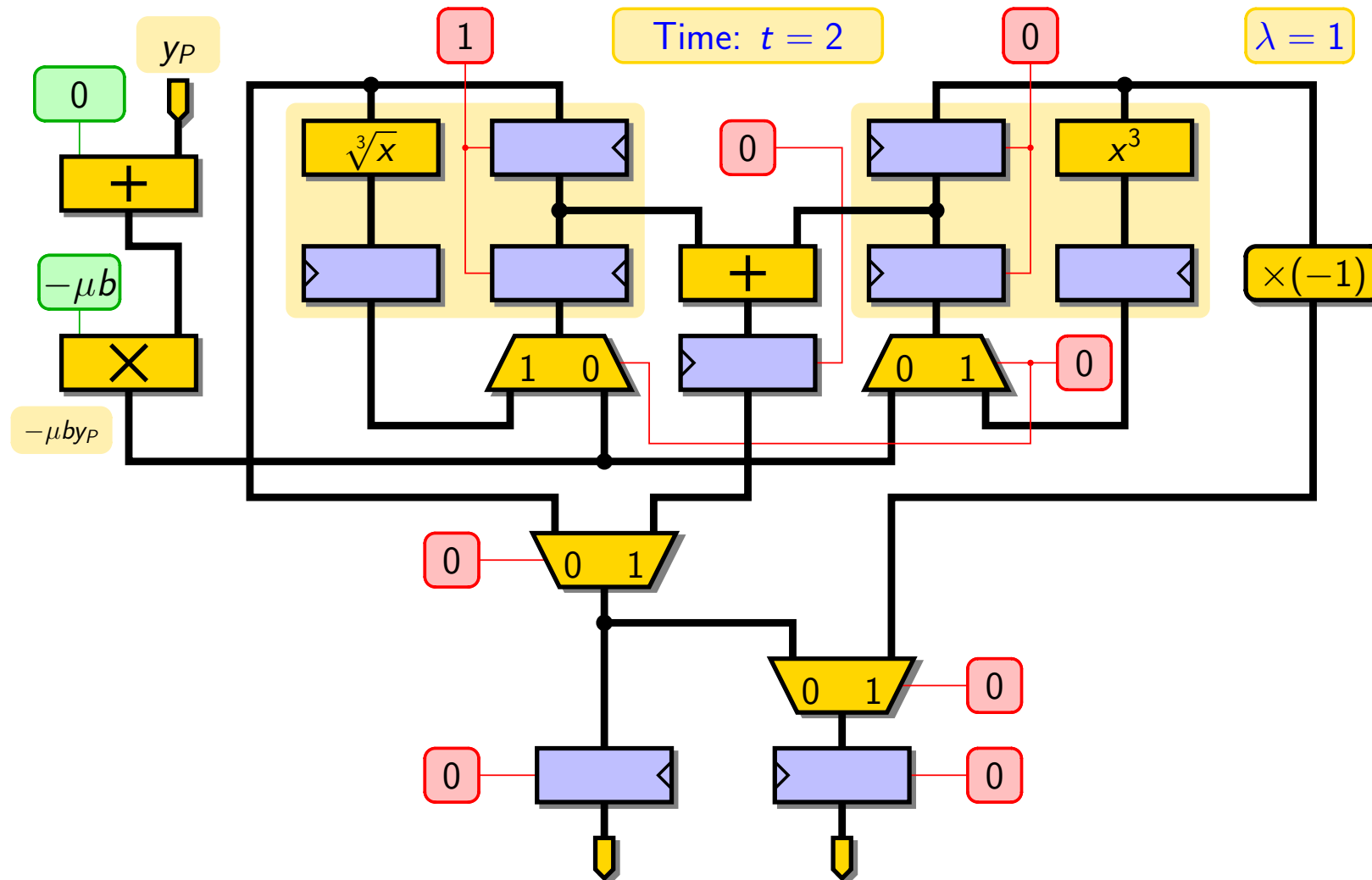
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



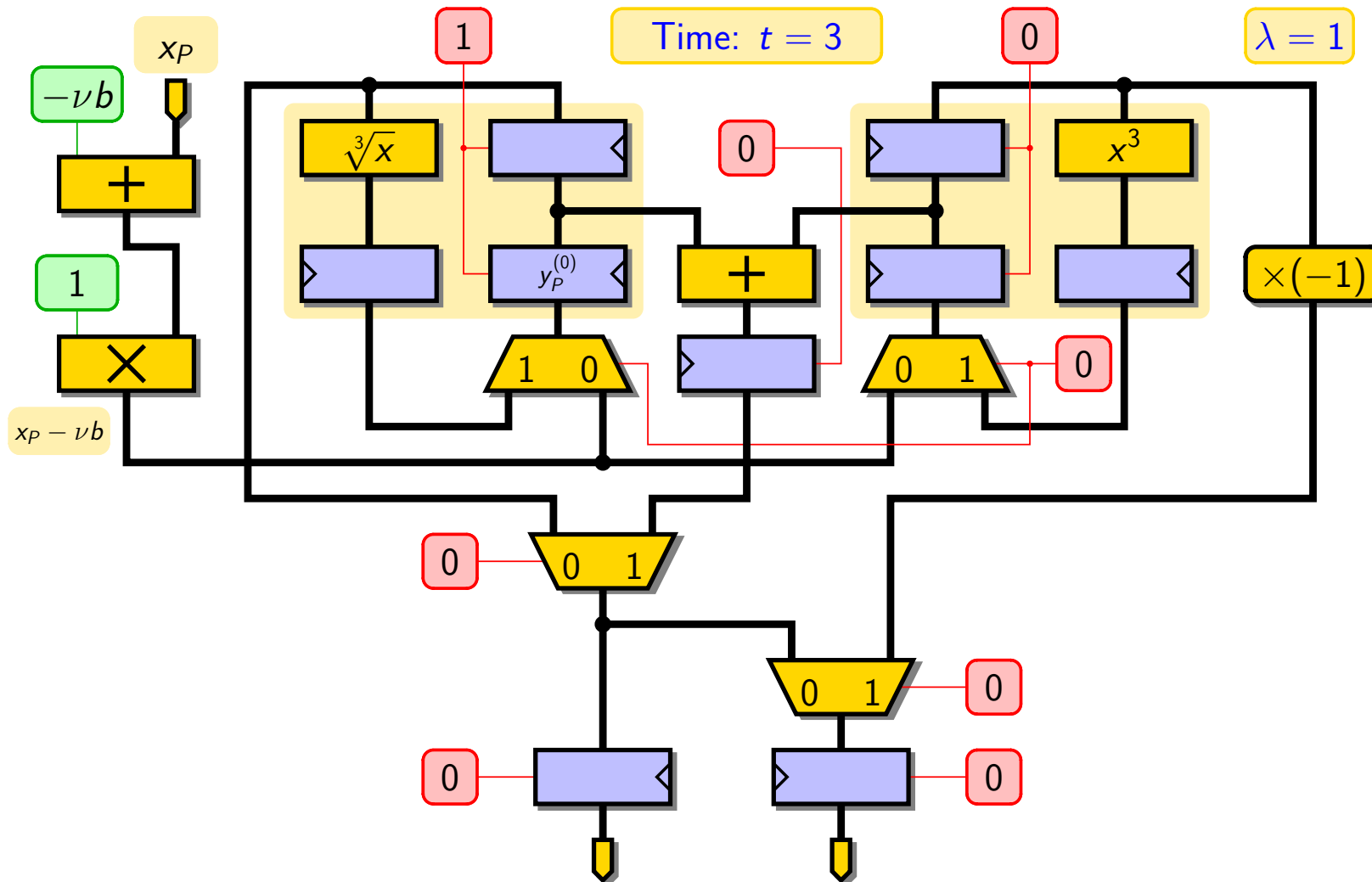
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



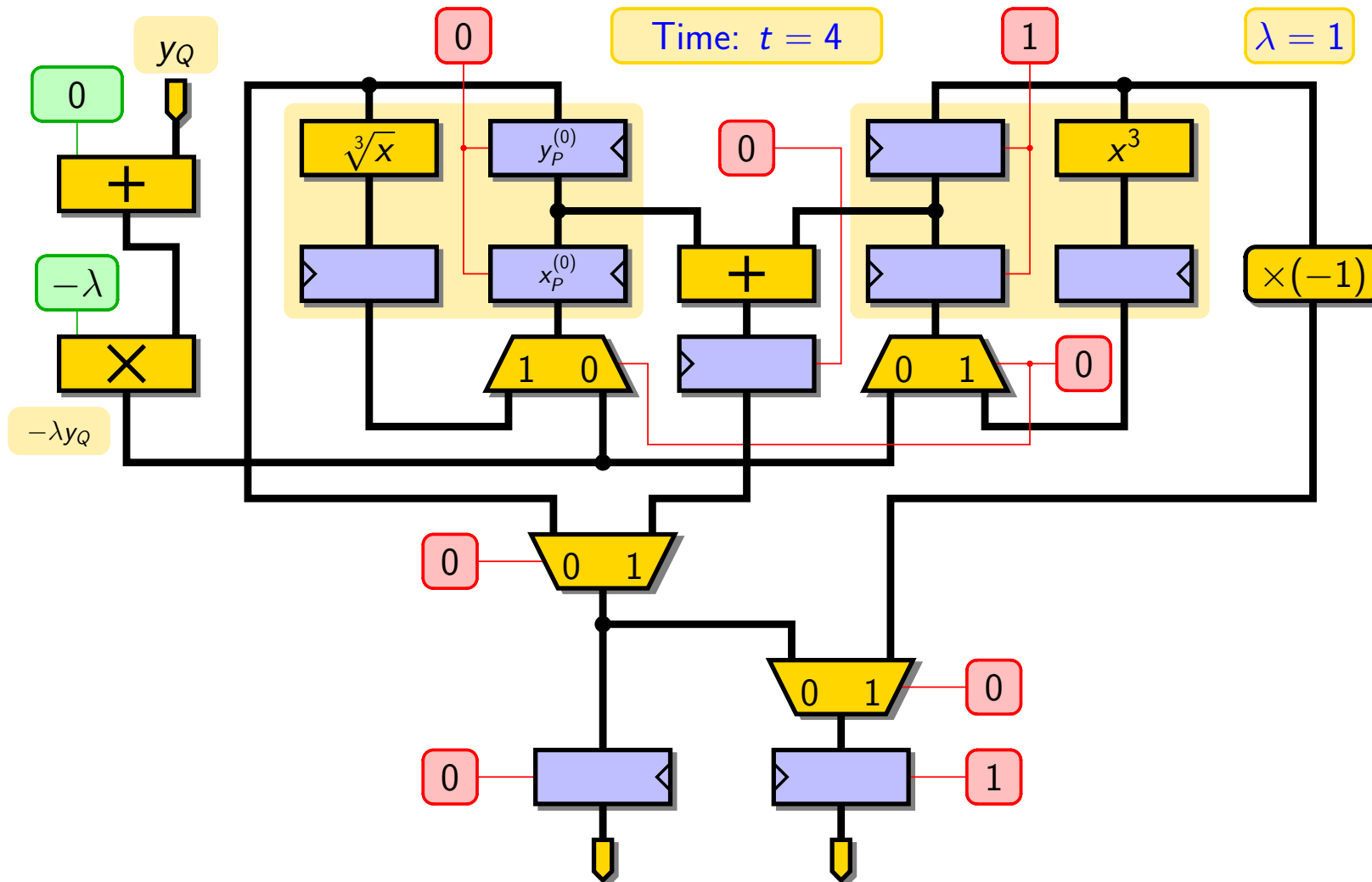
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



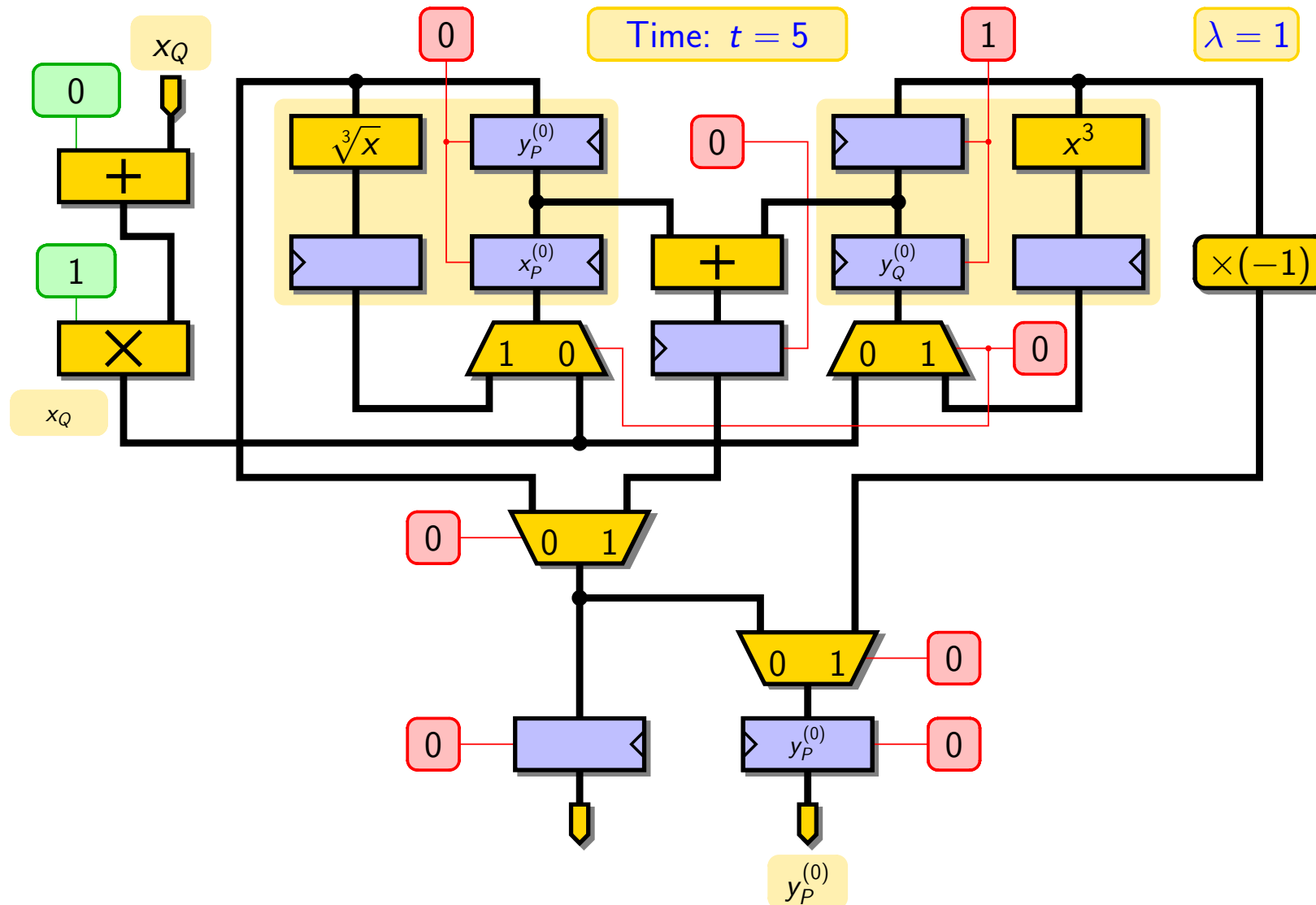
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



# Update of Coordinates of Points P and Q ( $\lambda = 1$ )

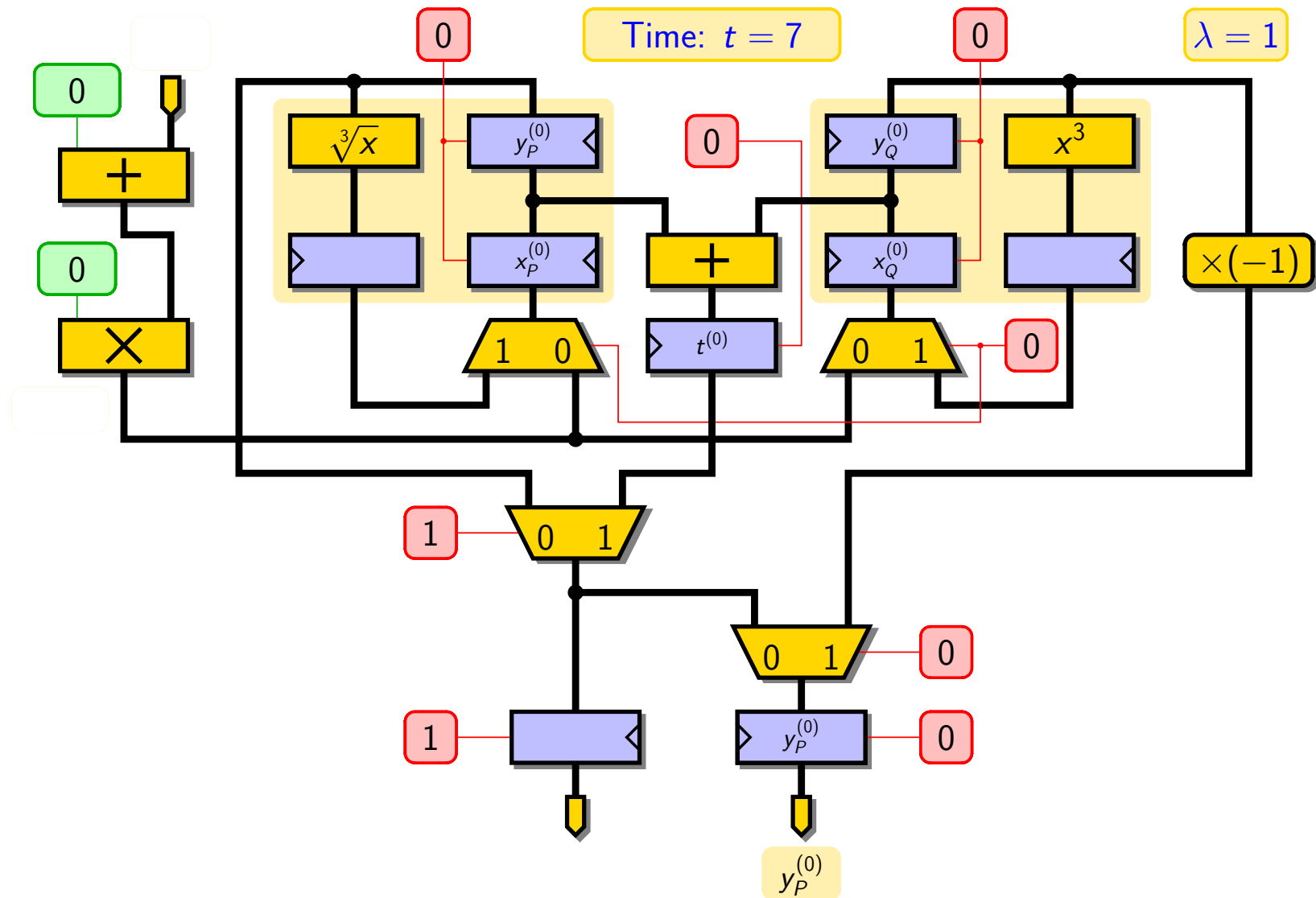


# Update of Coordinates of Points P and Q ( $\lambda = 1$ )

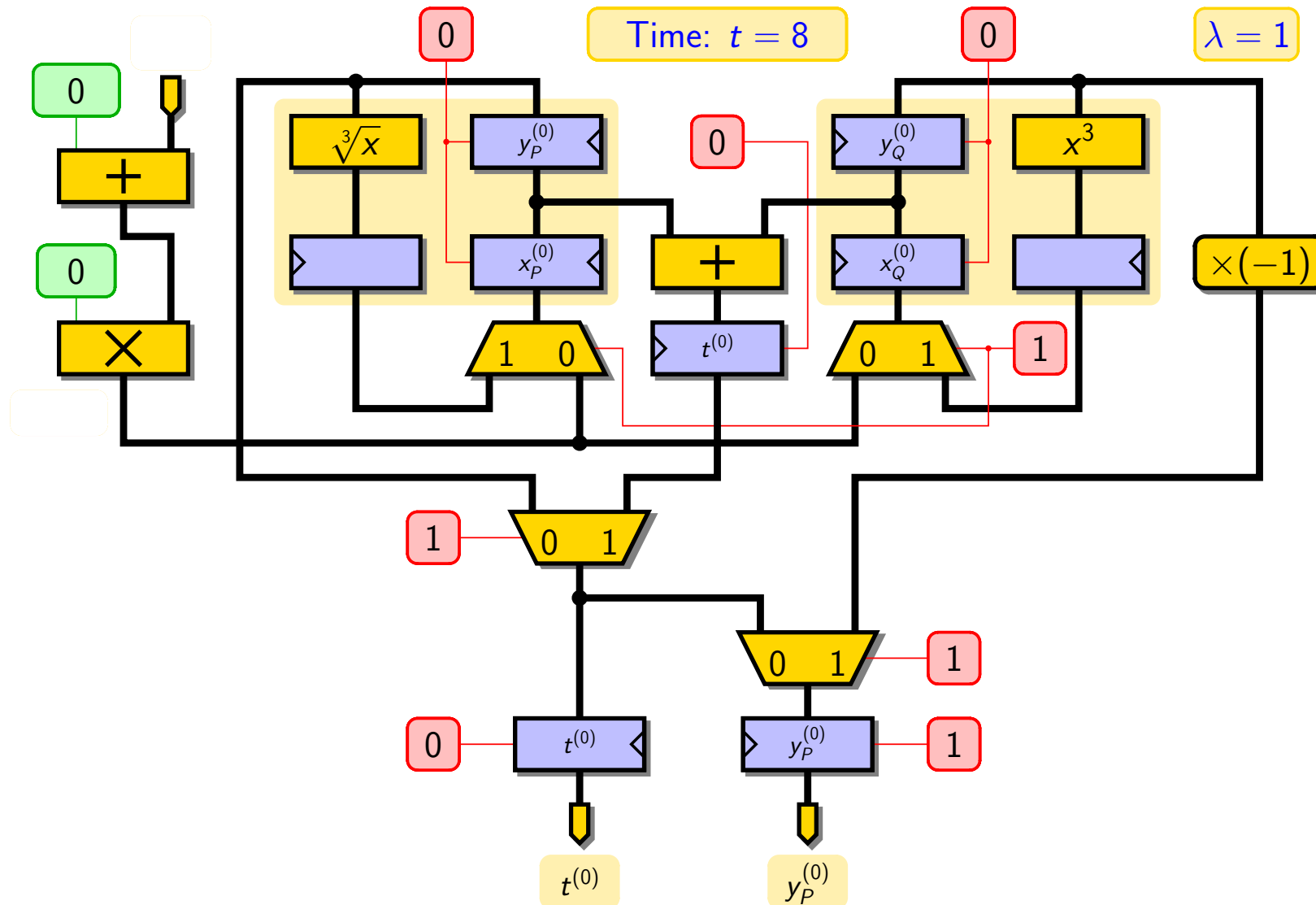




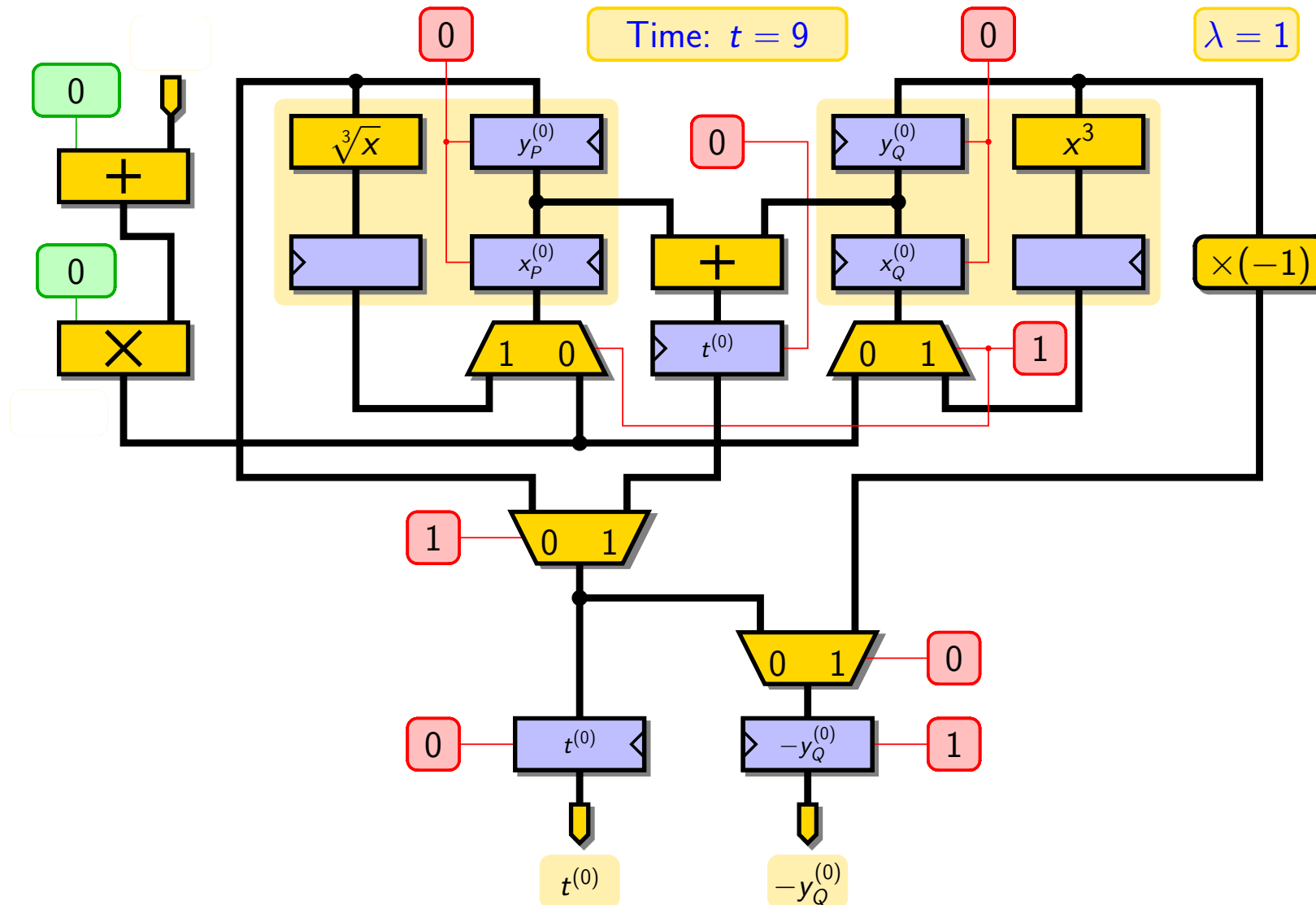
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



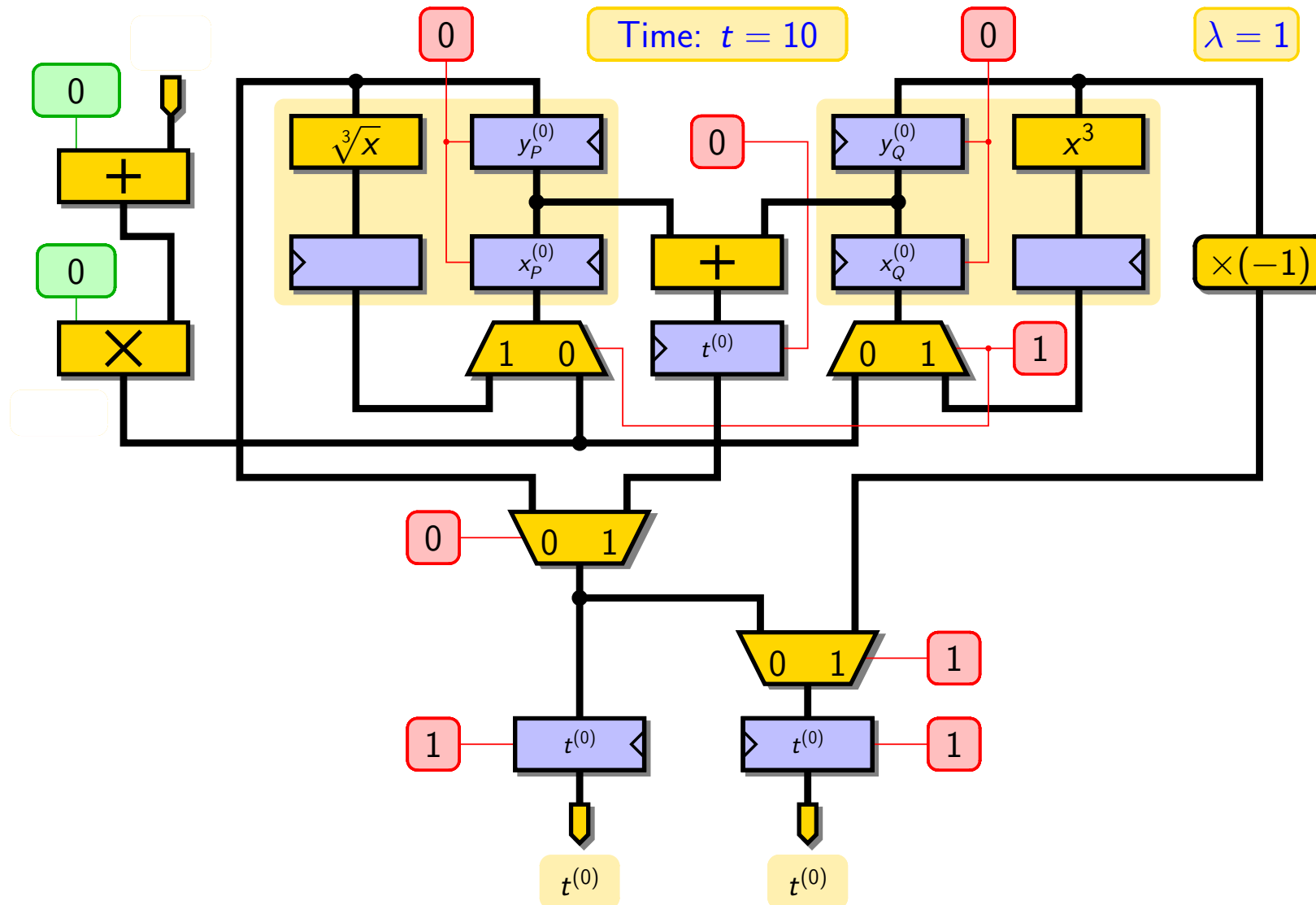
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



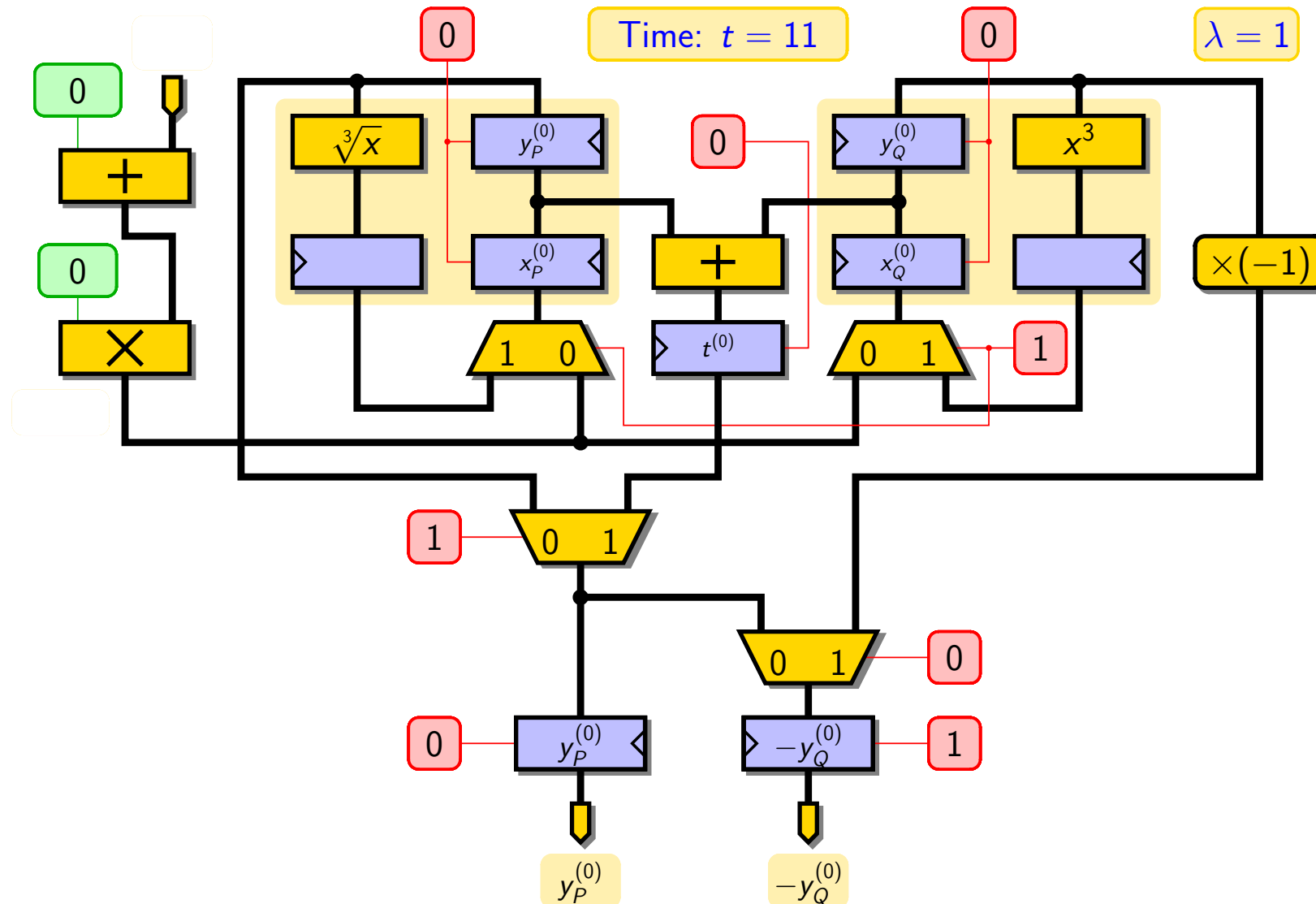
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



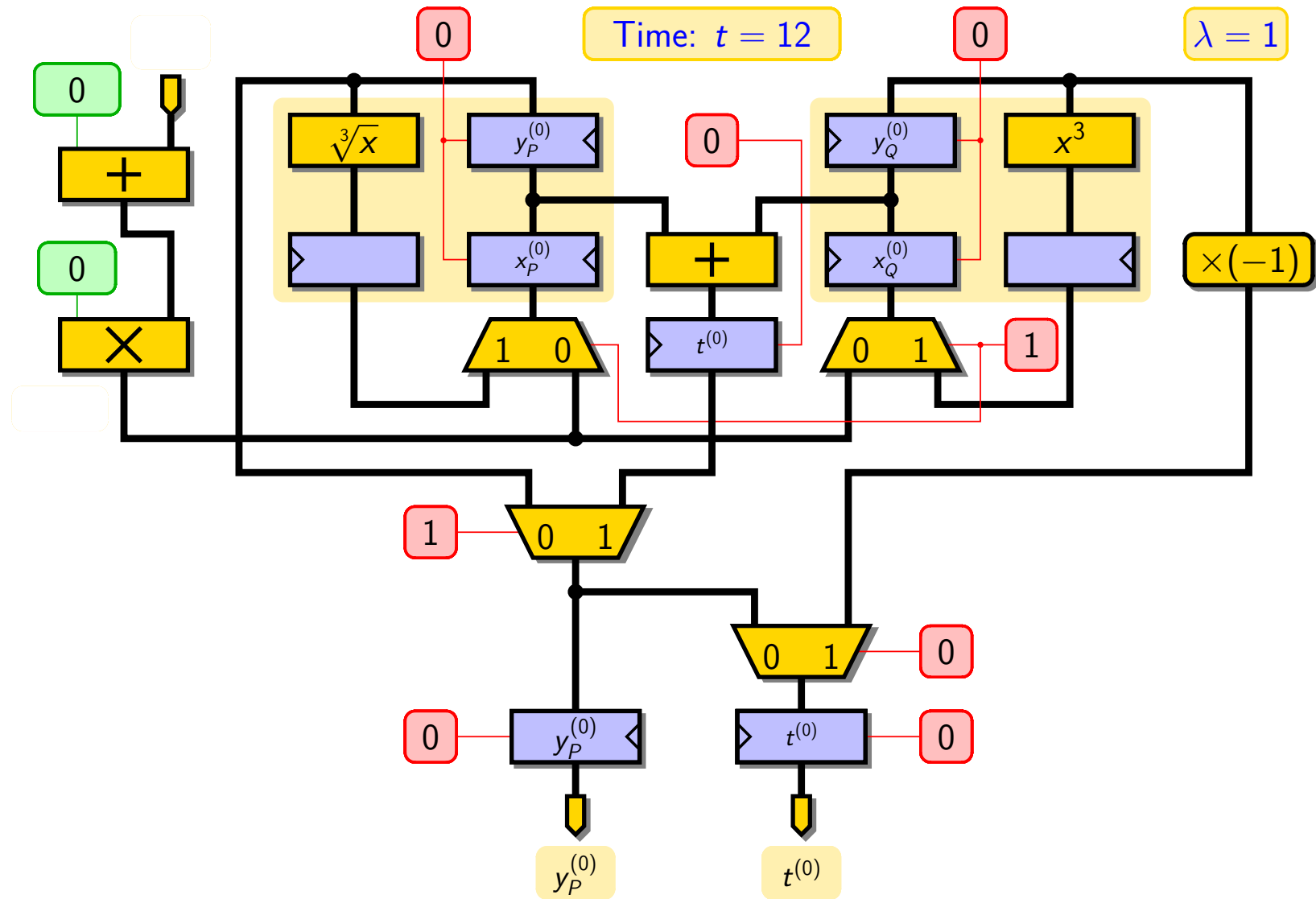
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



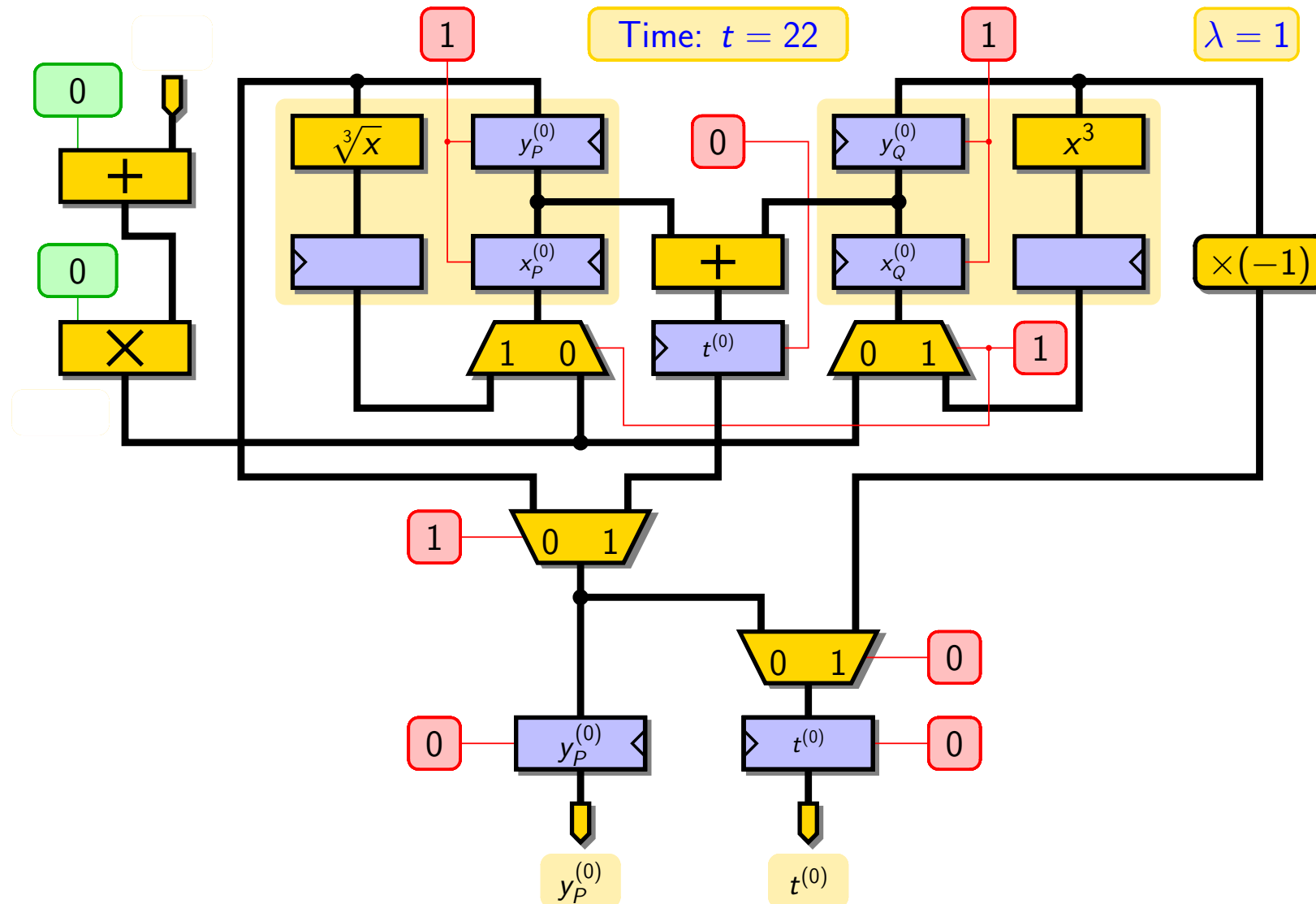
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



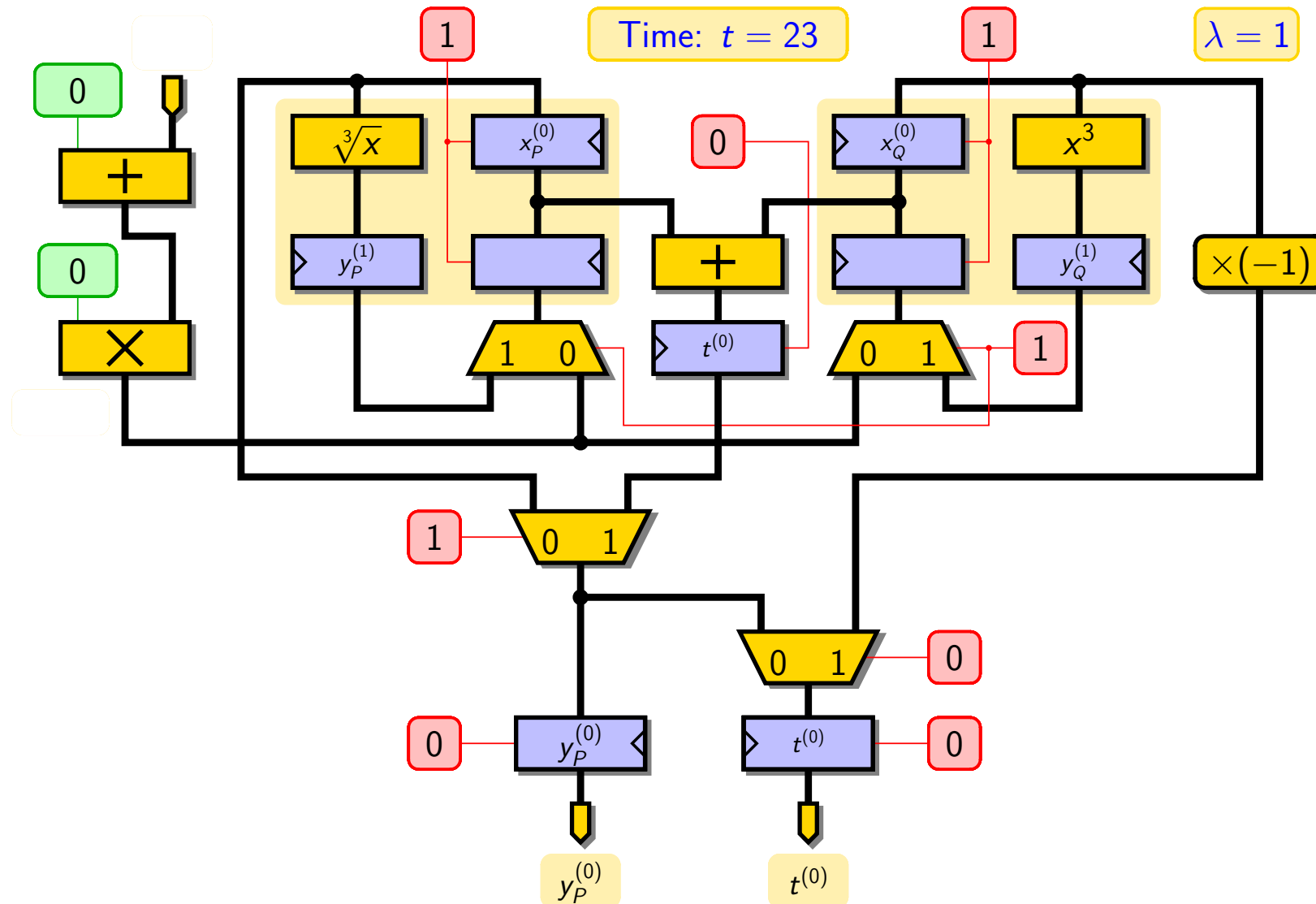
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



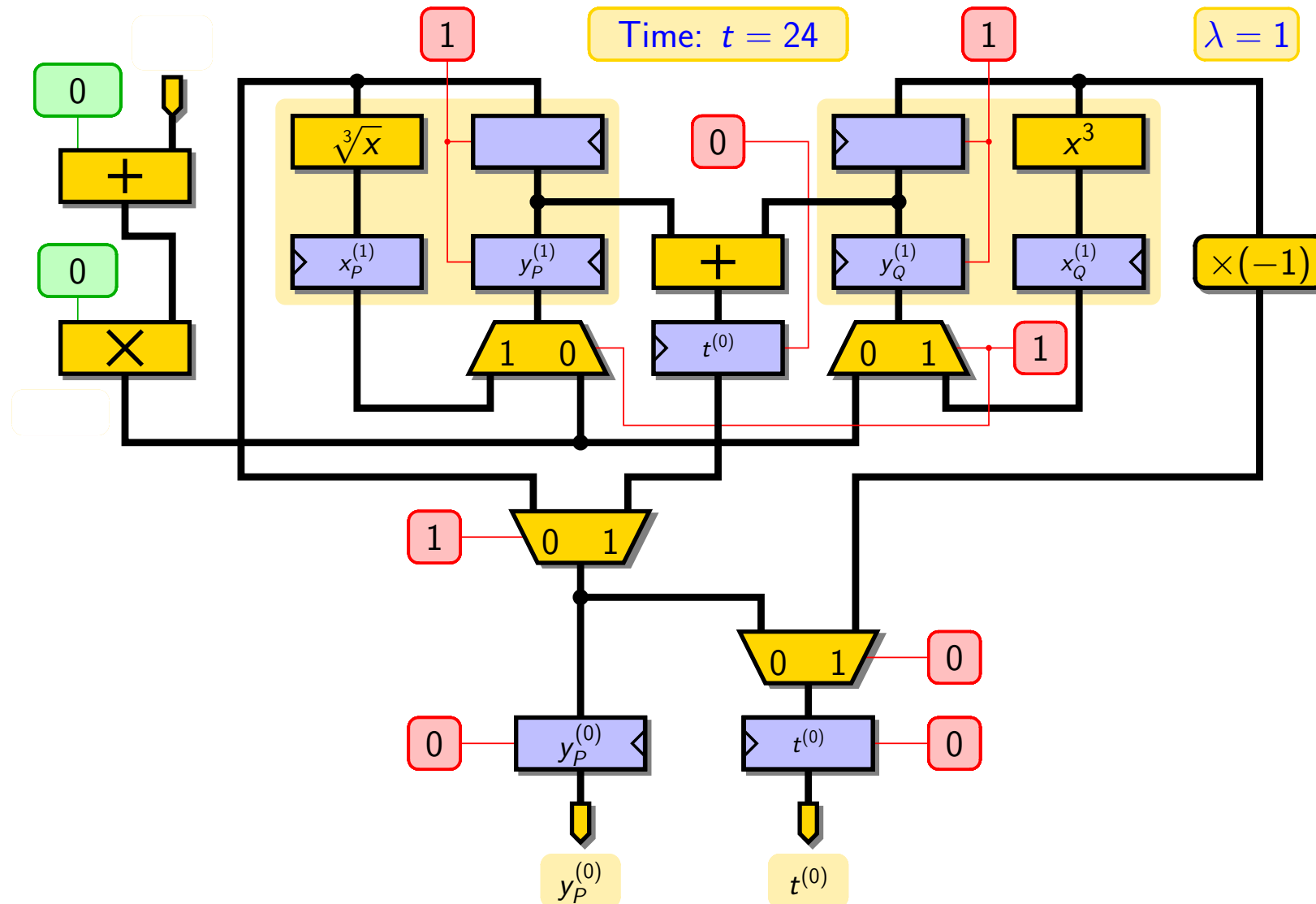
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



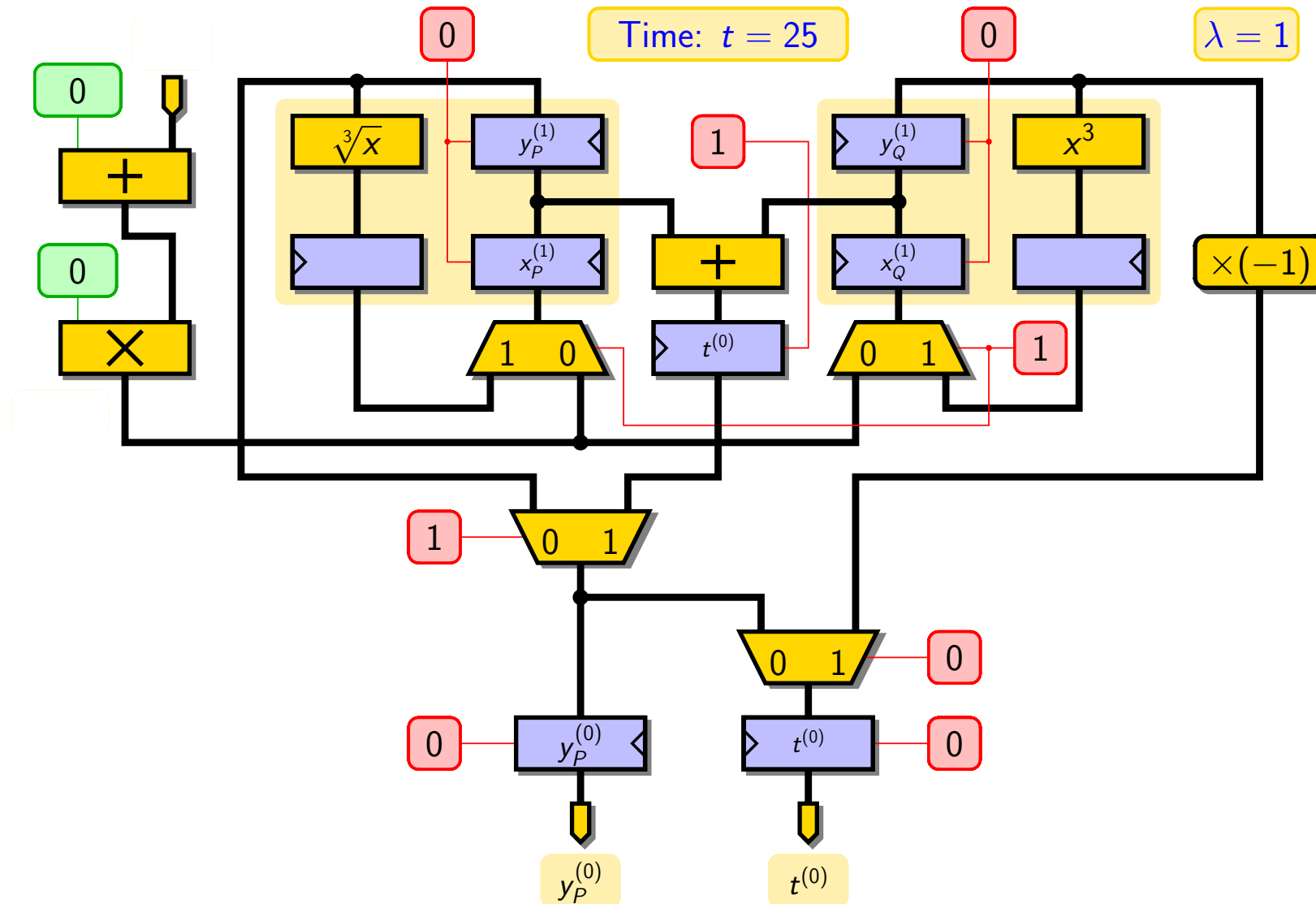
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



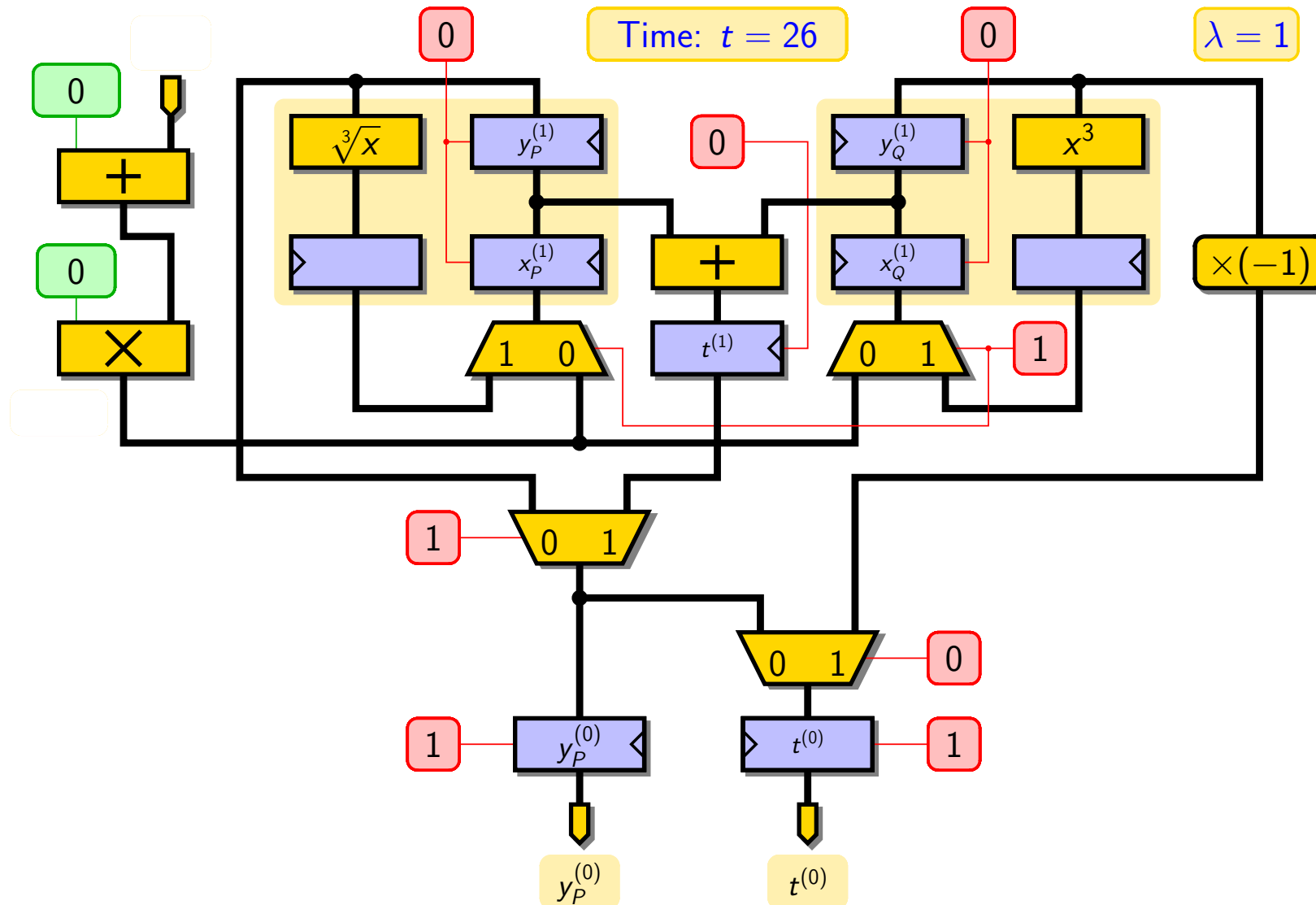
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



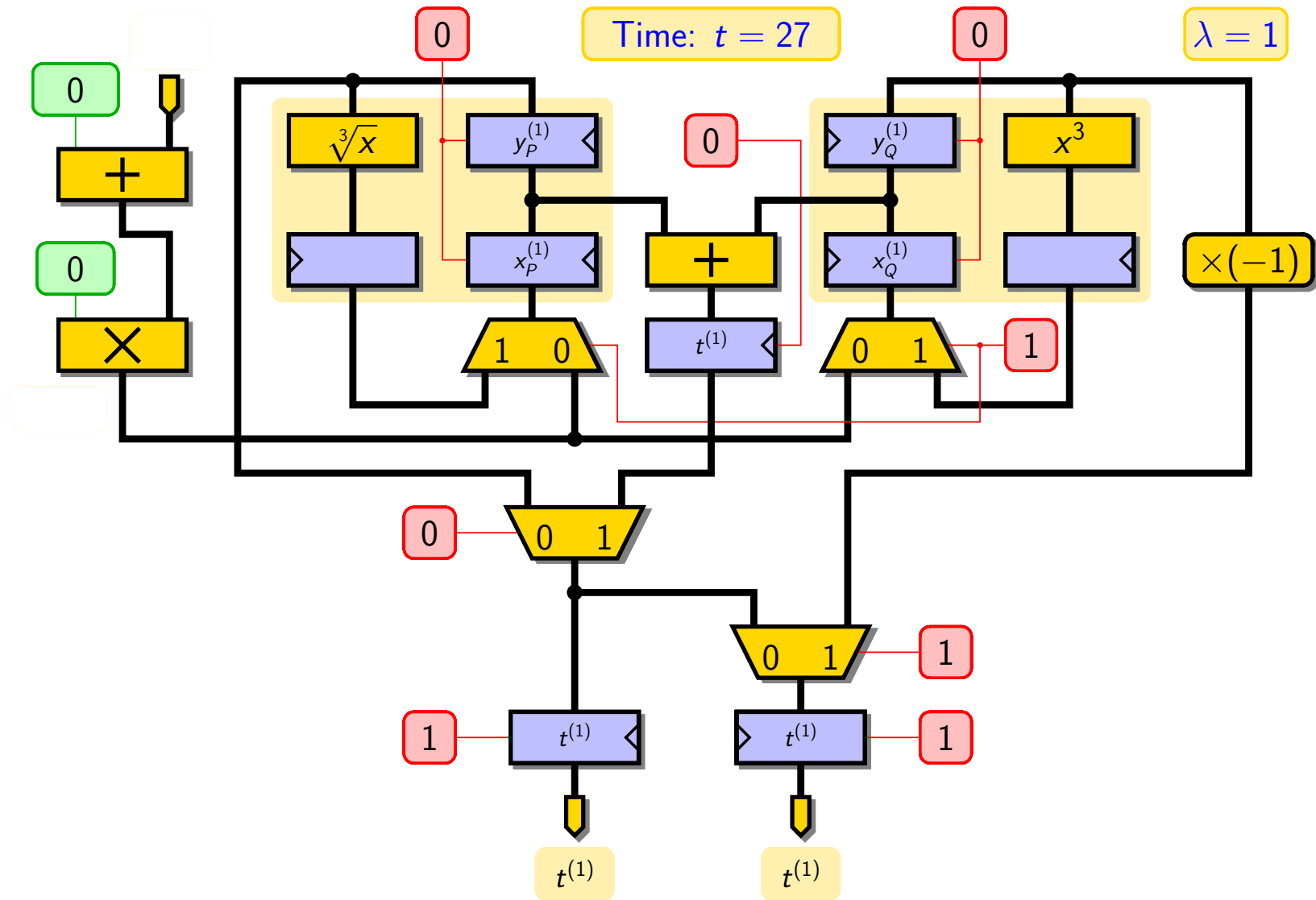
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



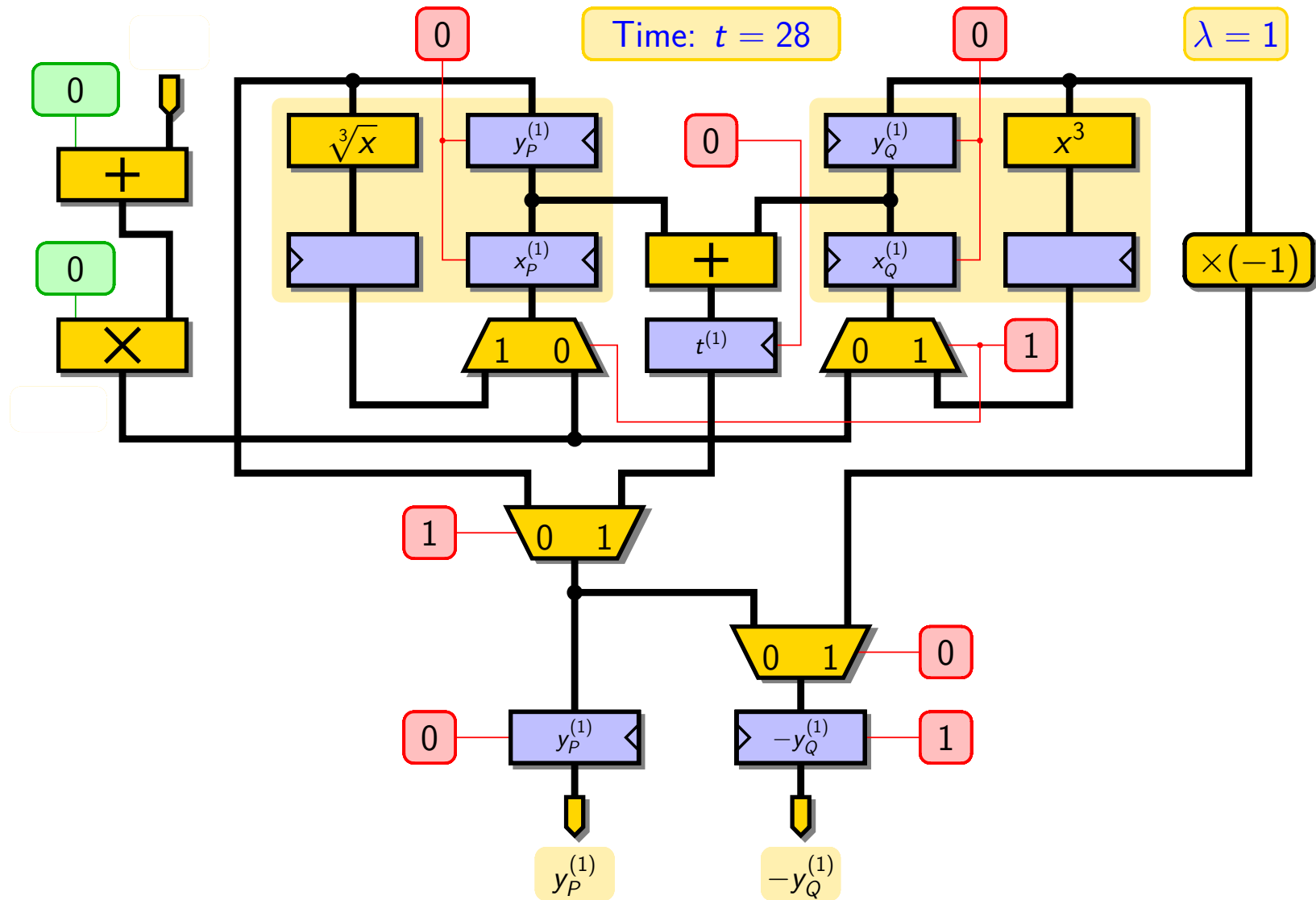
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



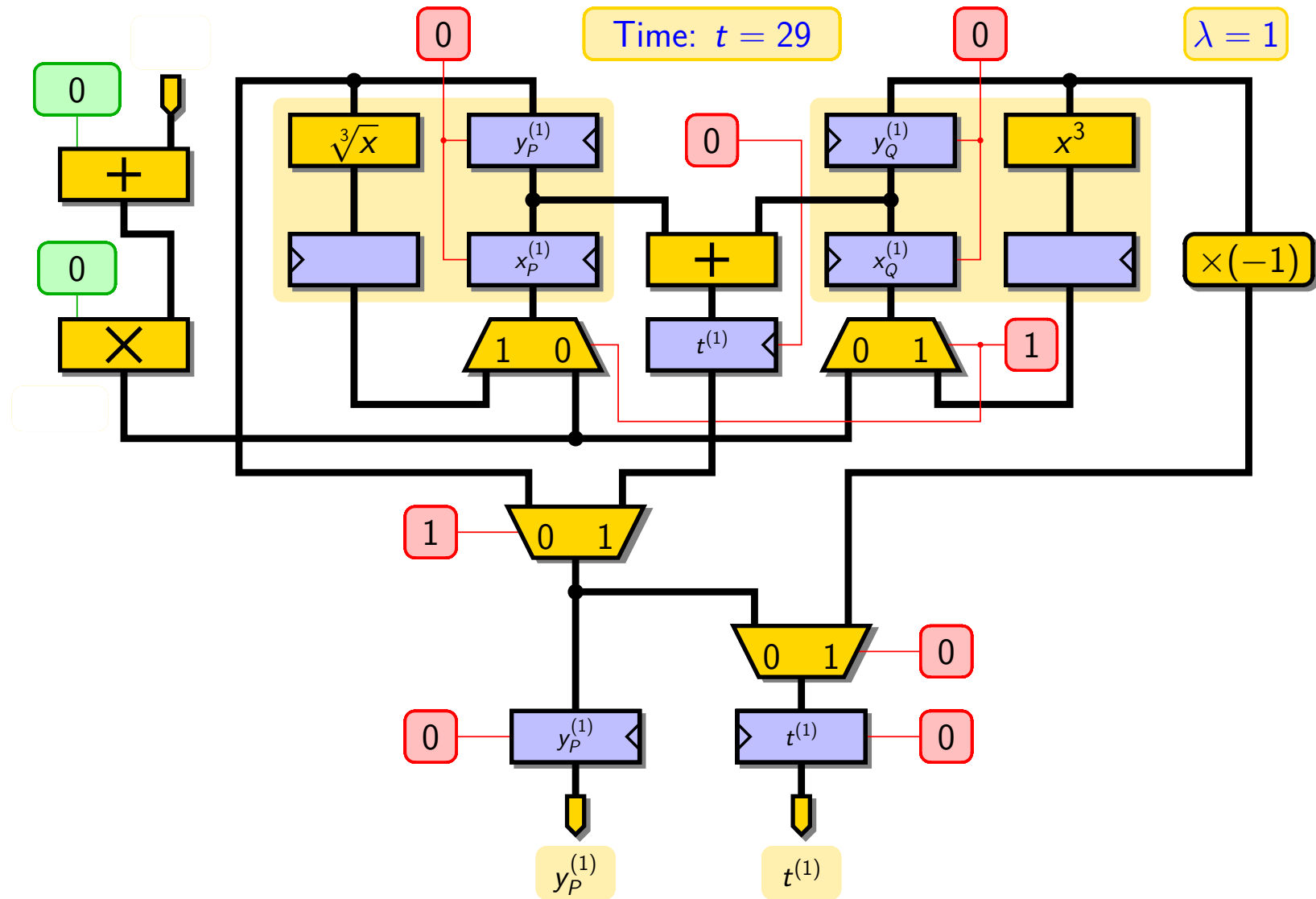
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



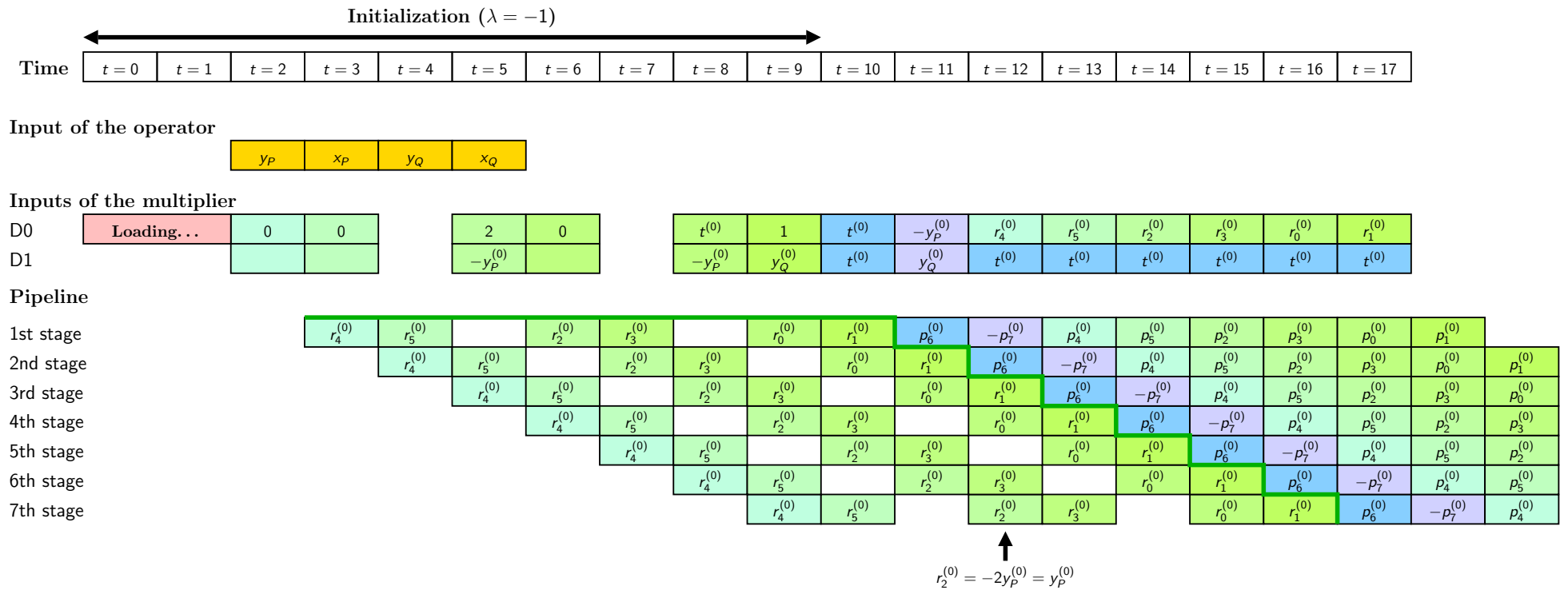
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



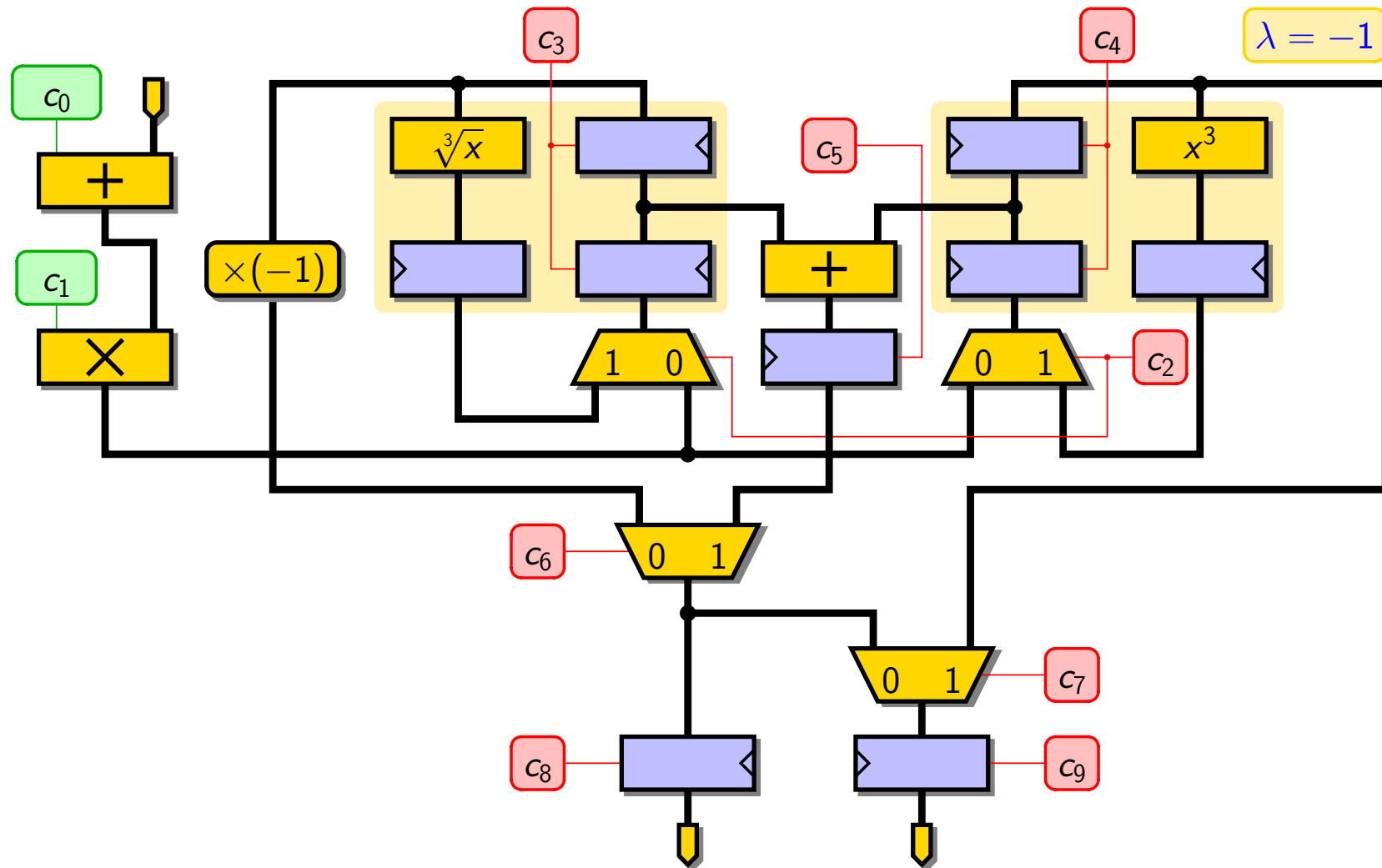
# Update of Coordinates of Points P and Q ( $\lambda = 1$ )



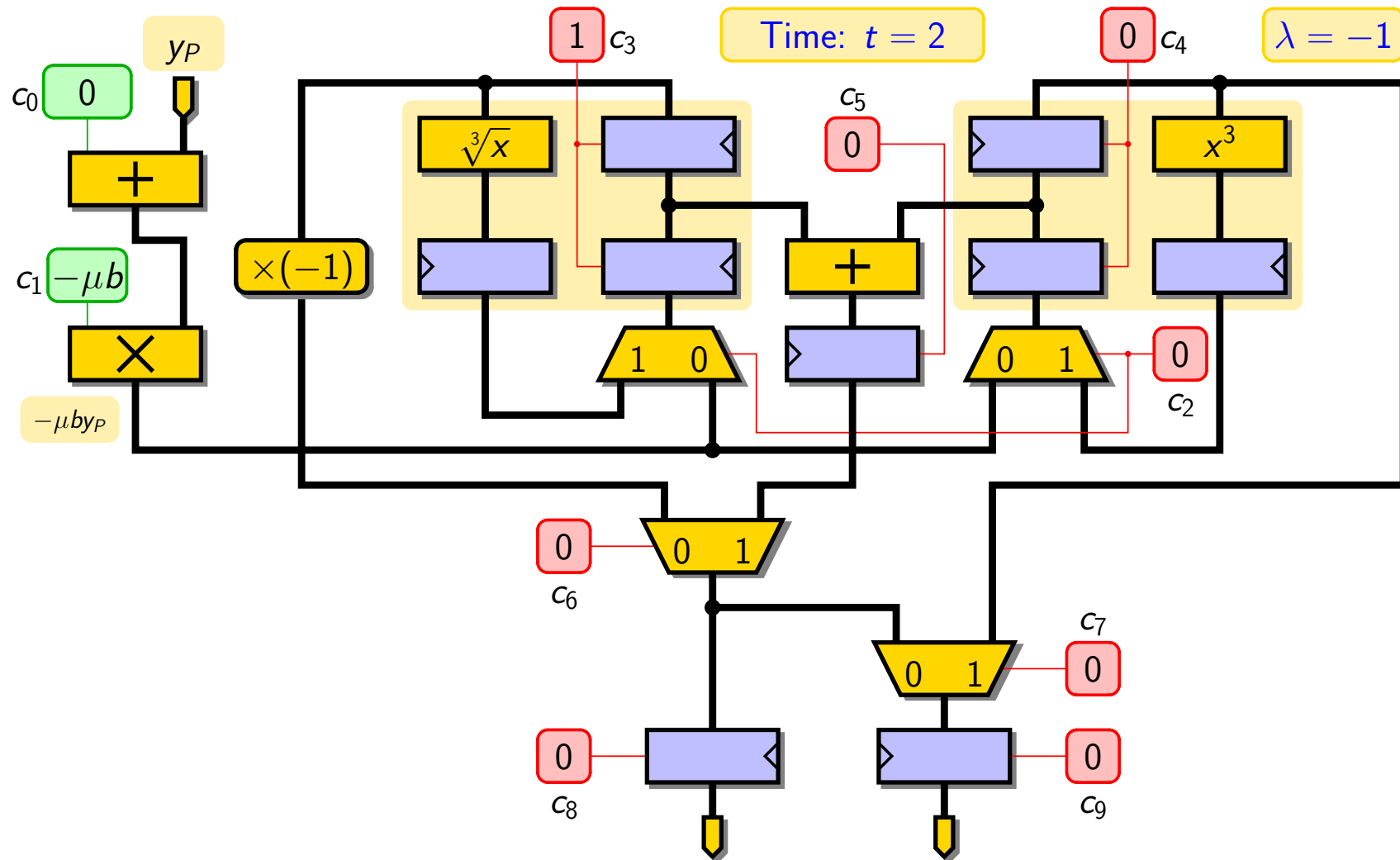
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



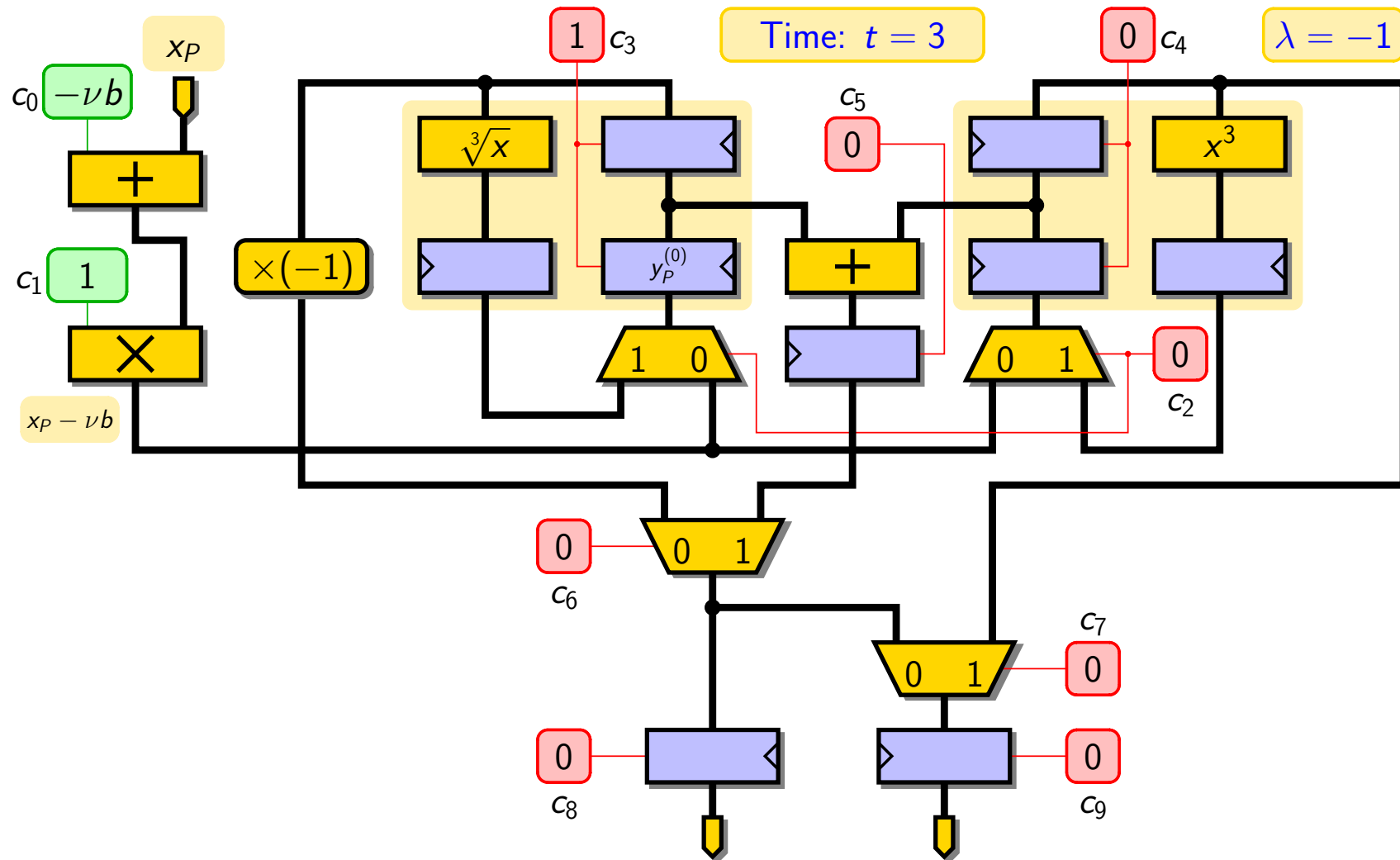
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



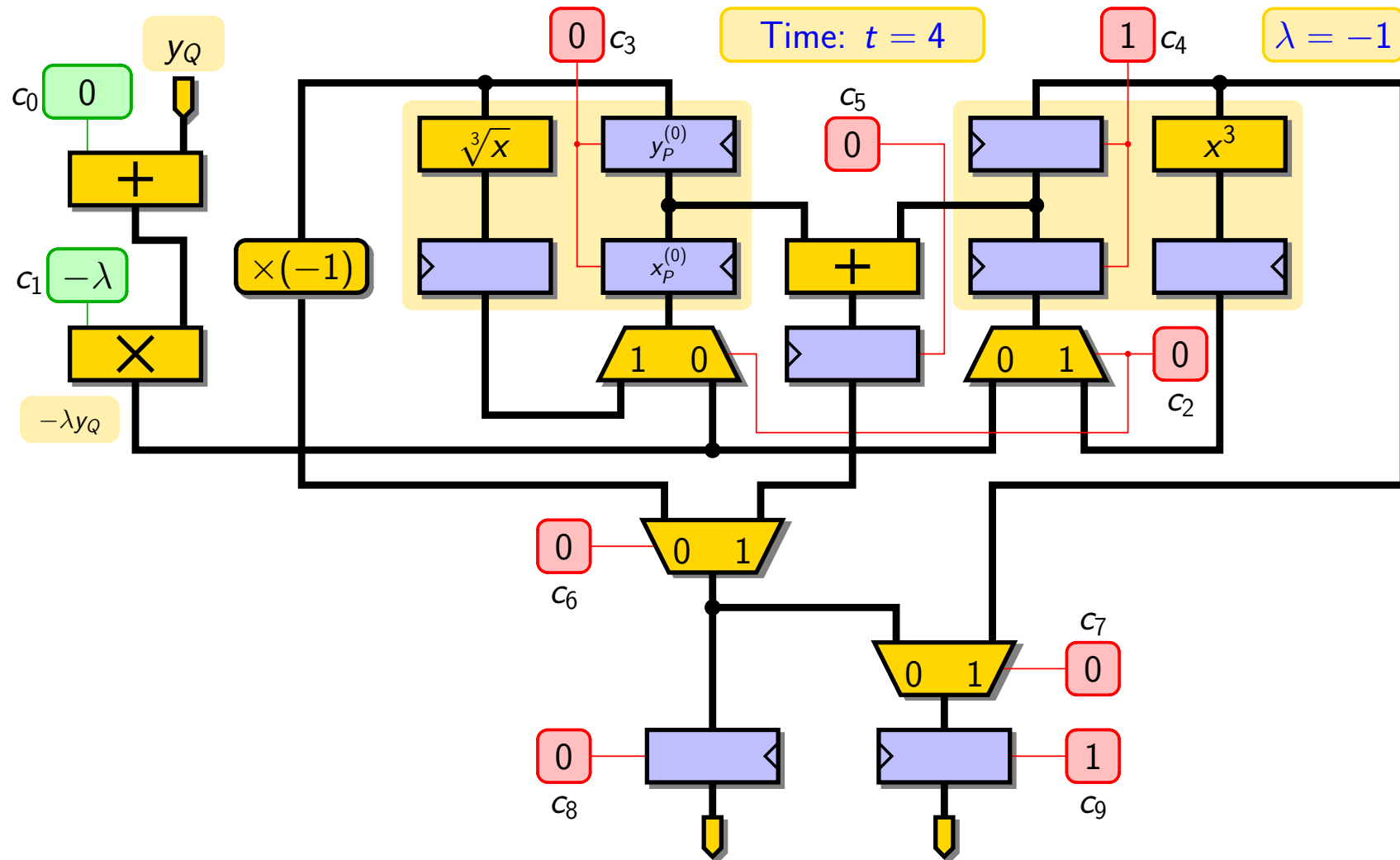
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



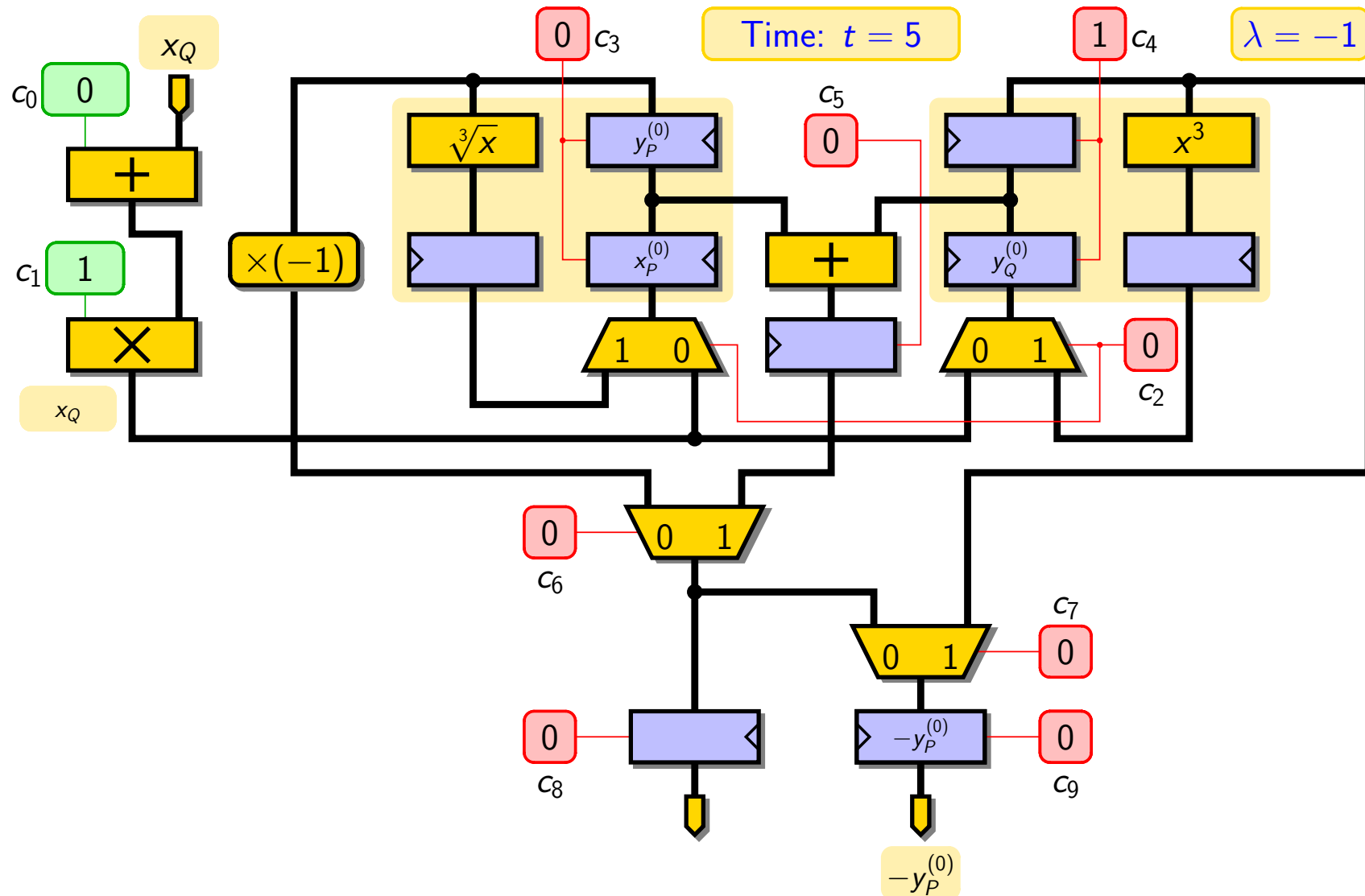
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



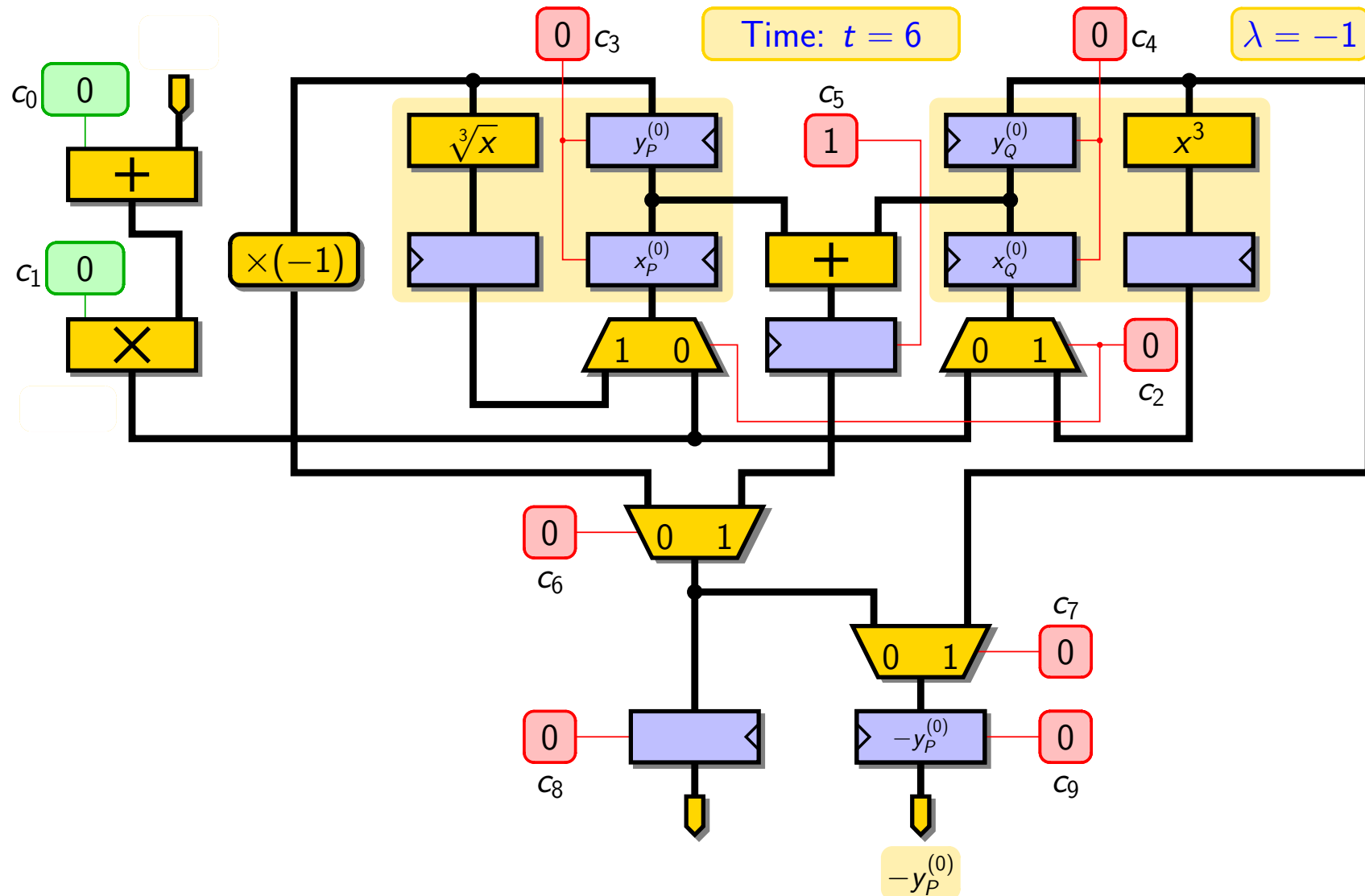
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



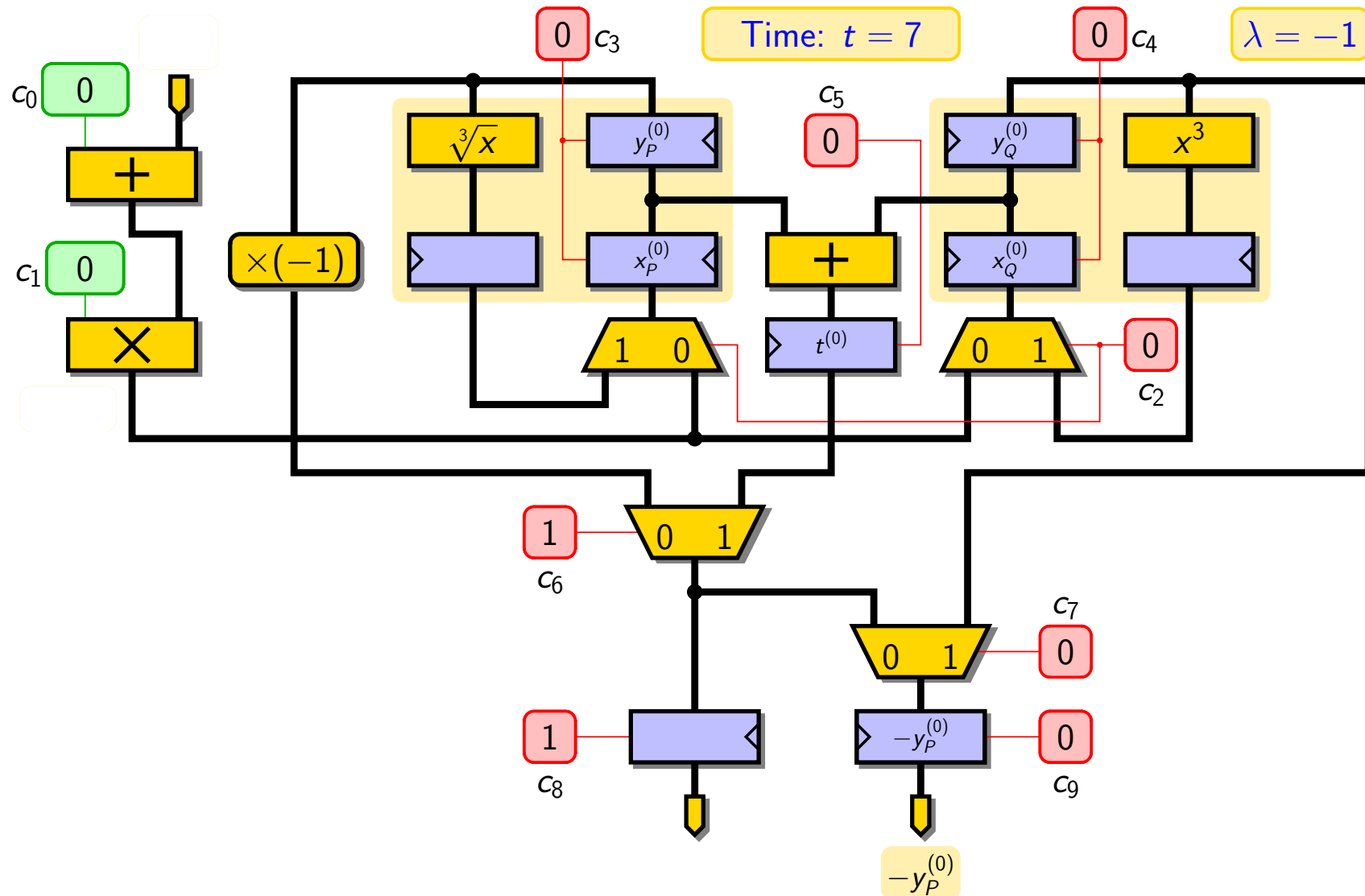
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



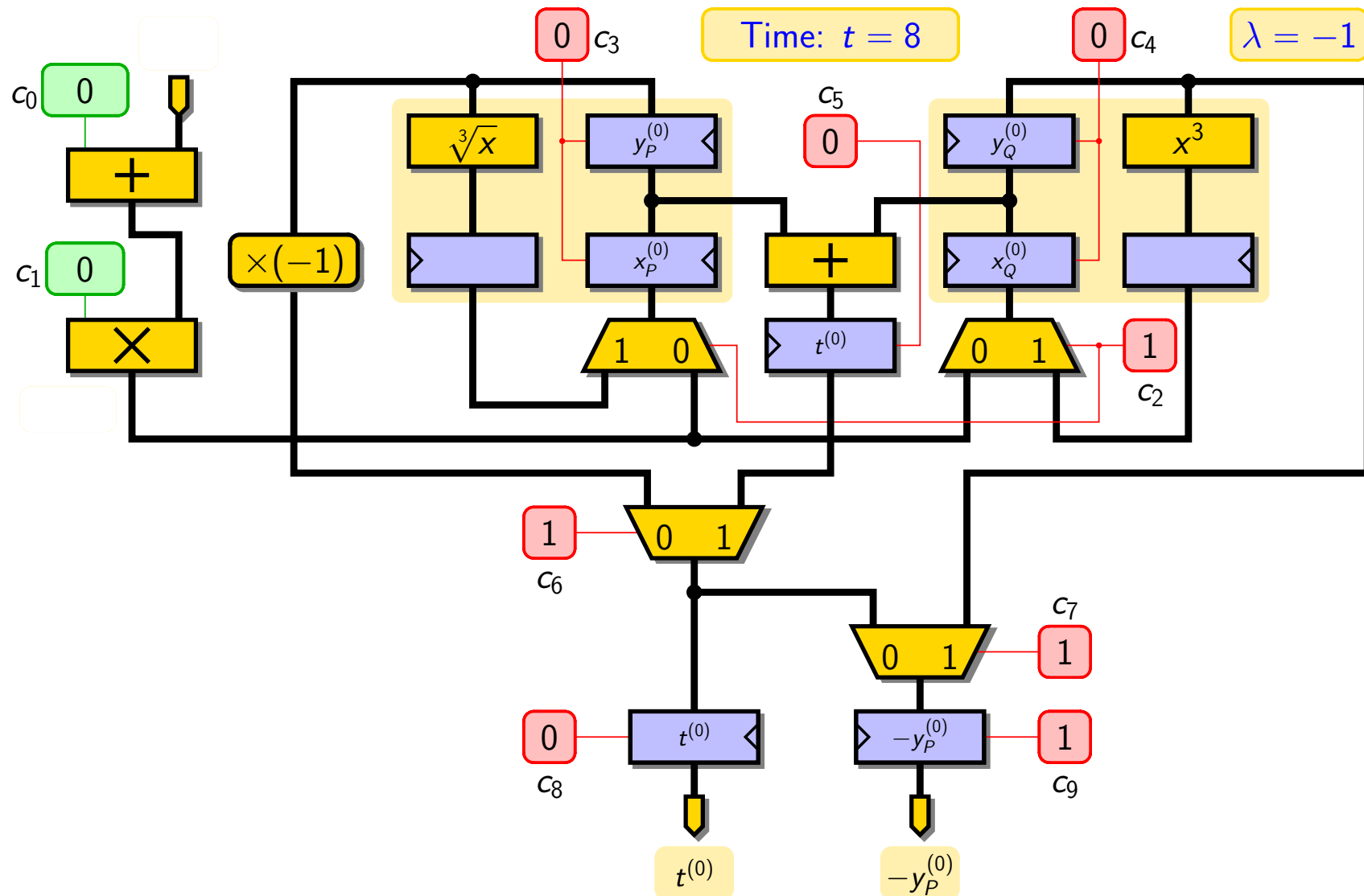
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



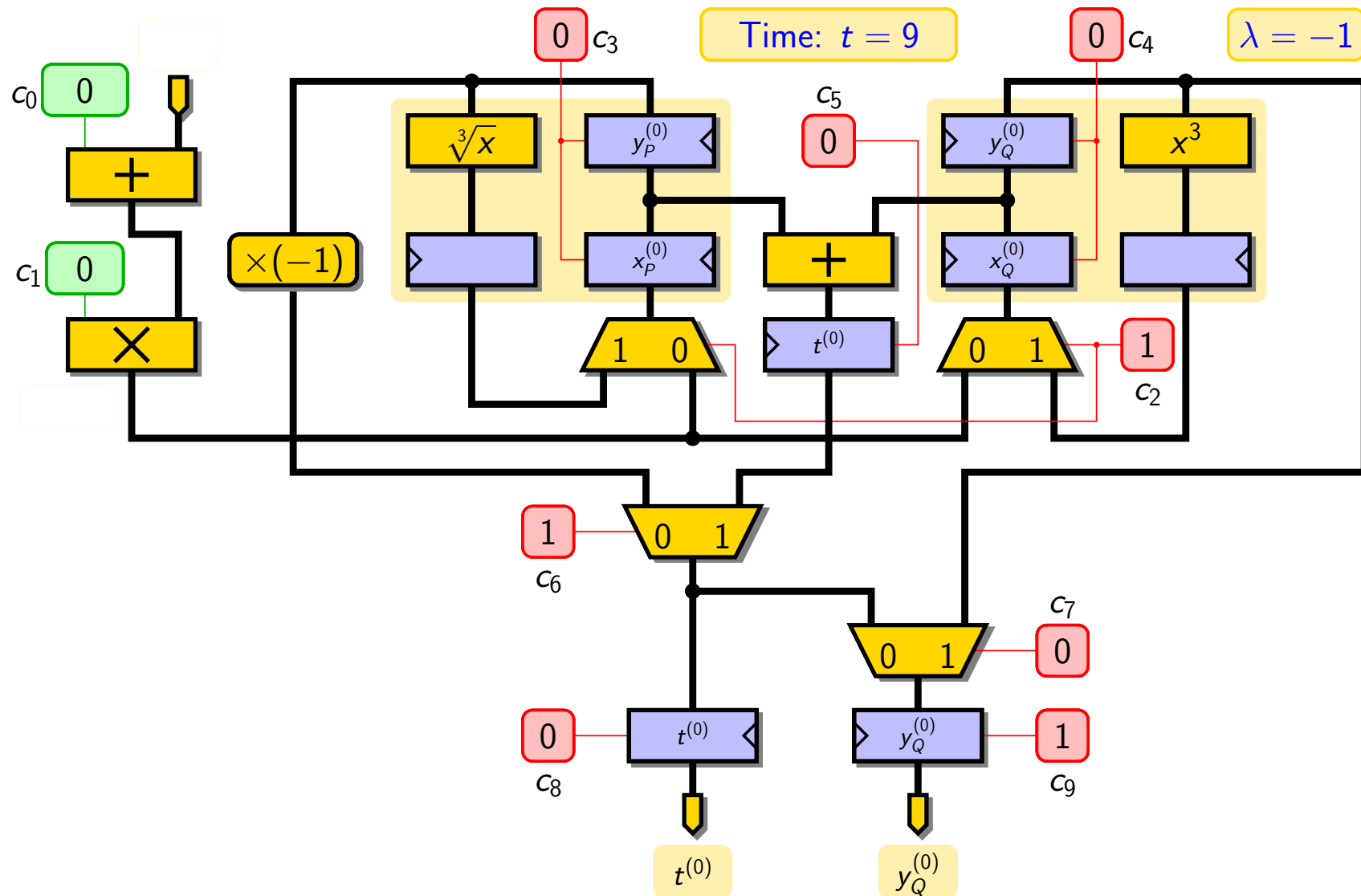
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



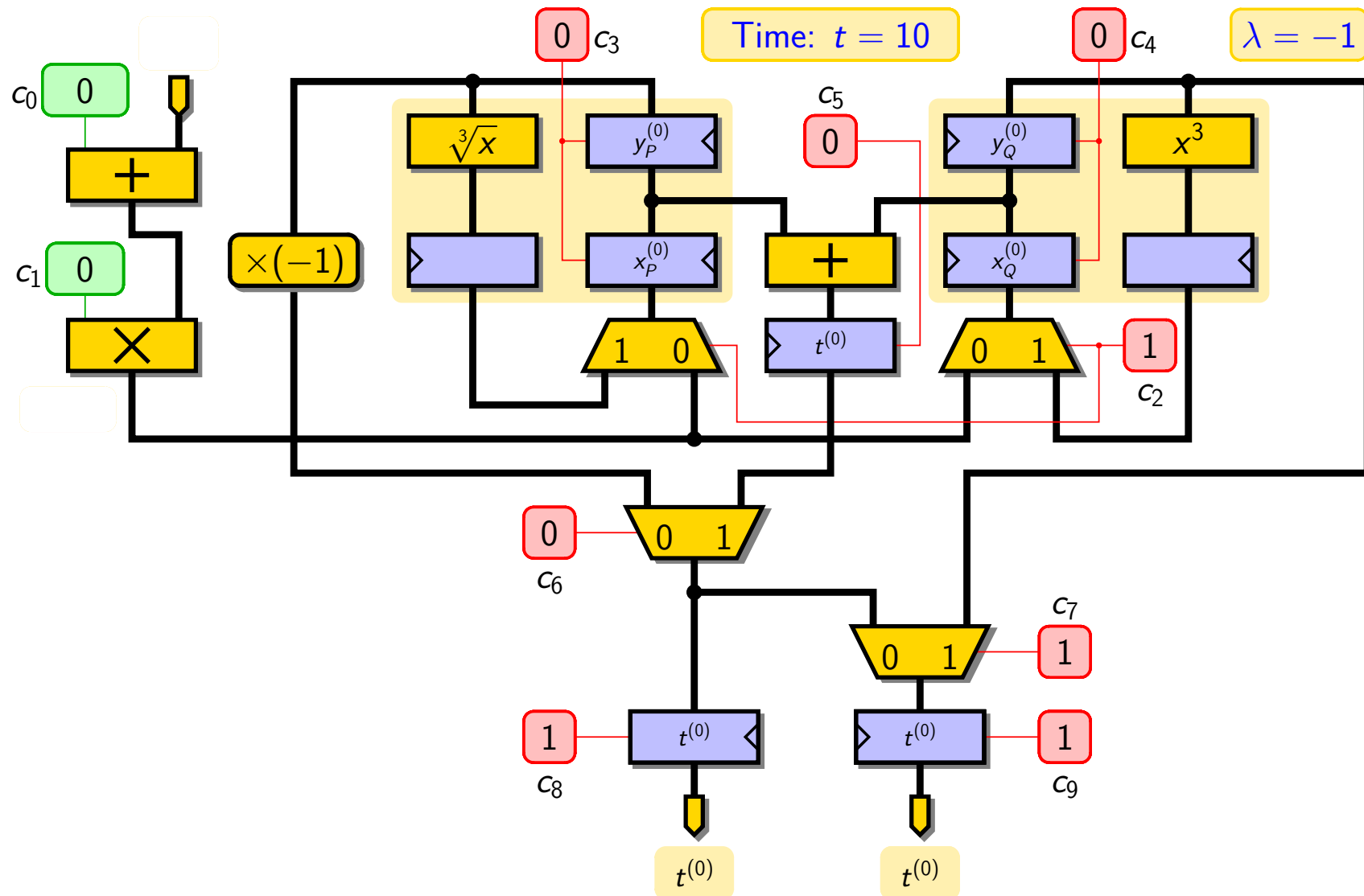
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



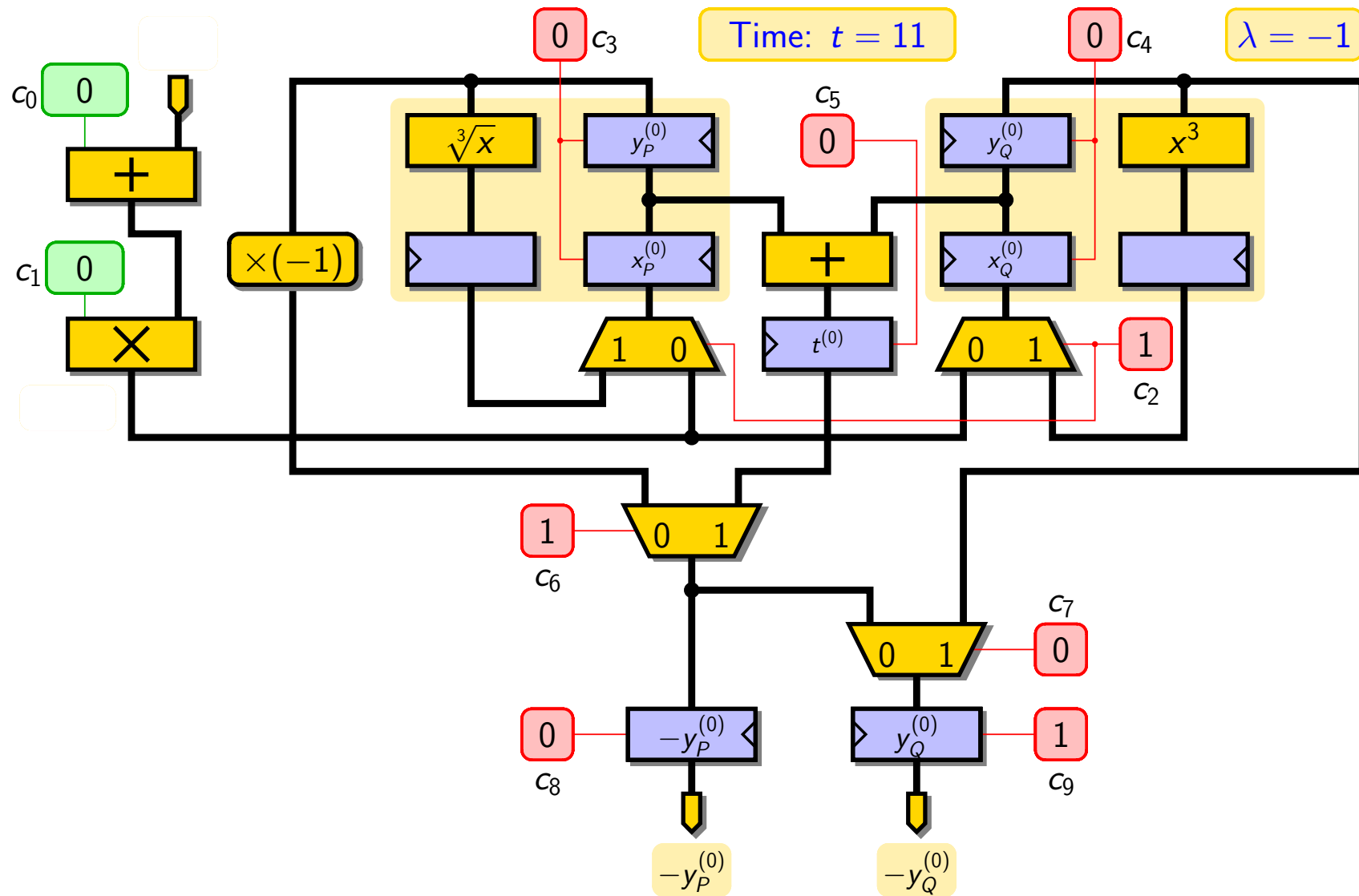
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



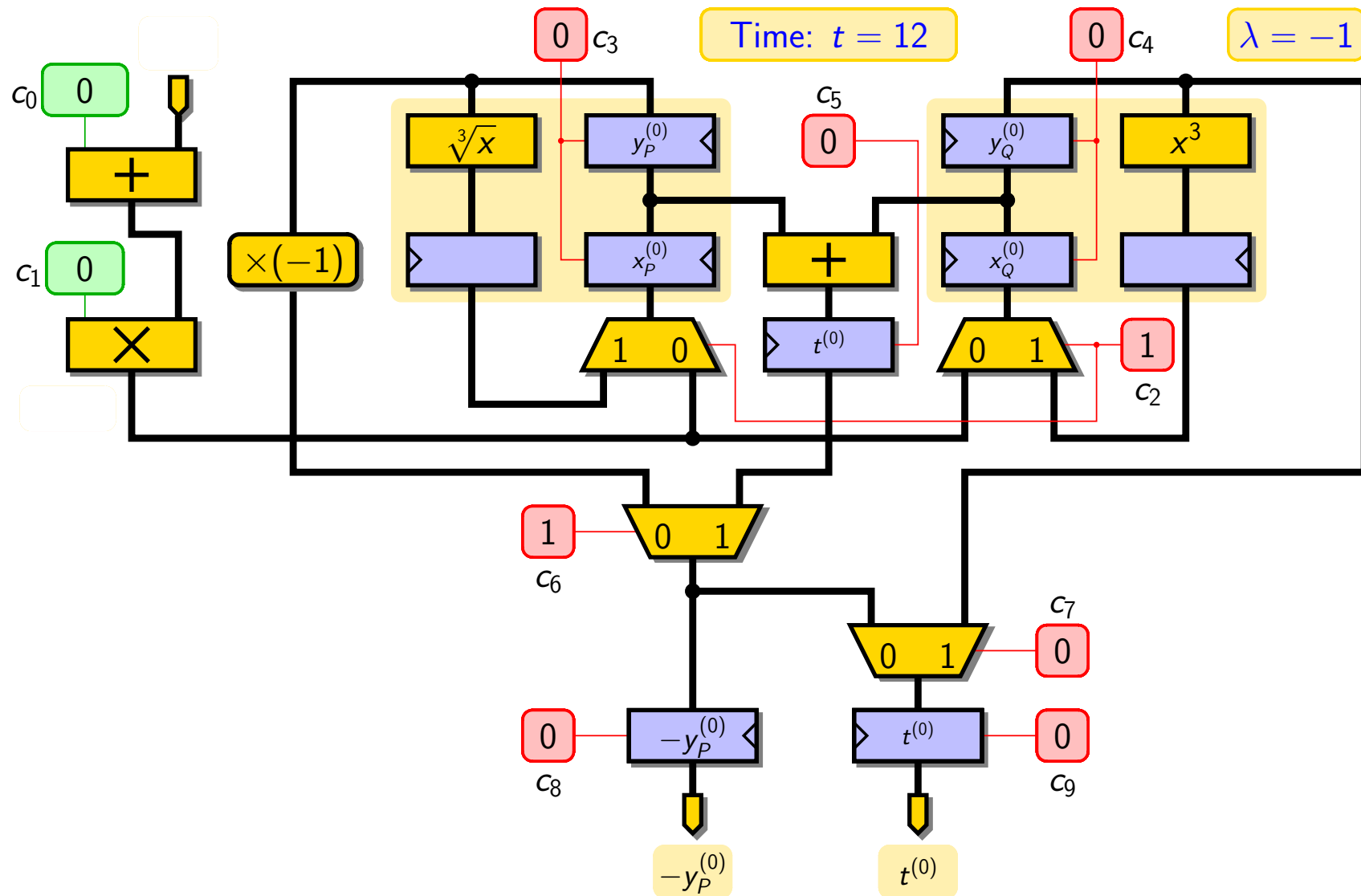
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



# Update of Coordinates of Points P and Q ( $\lambda = -1$ )

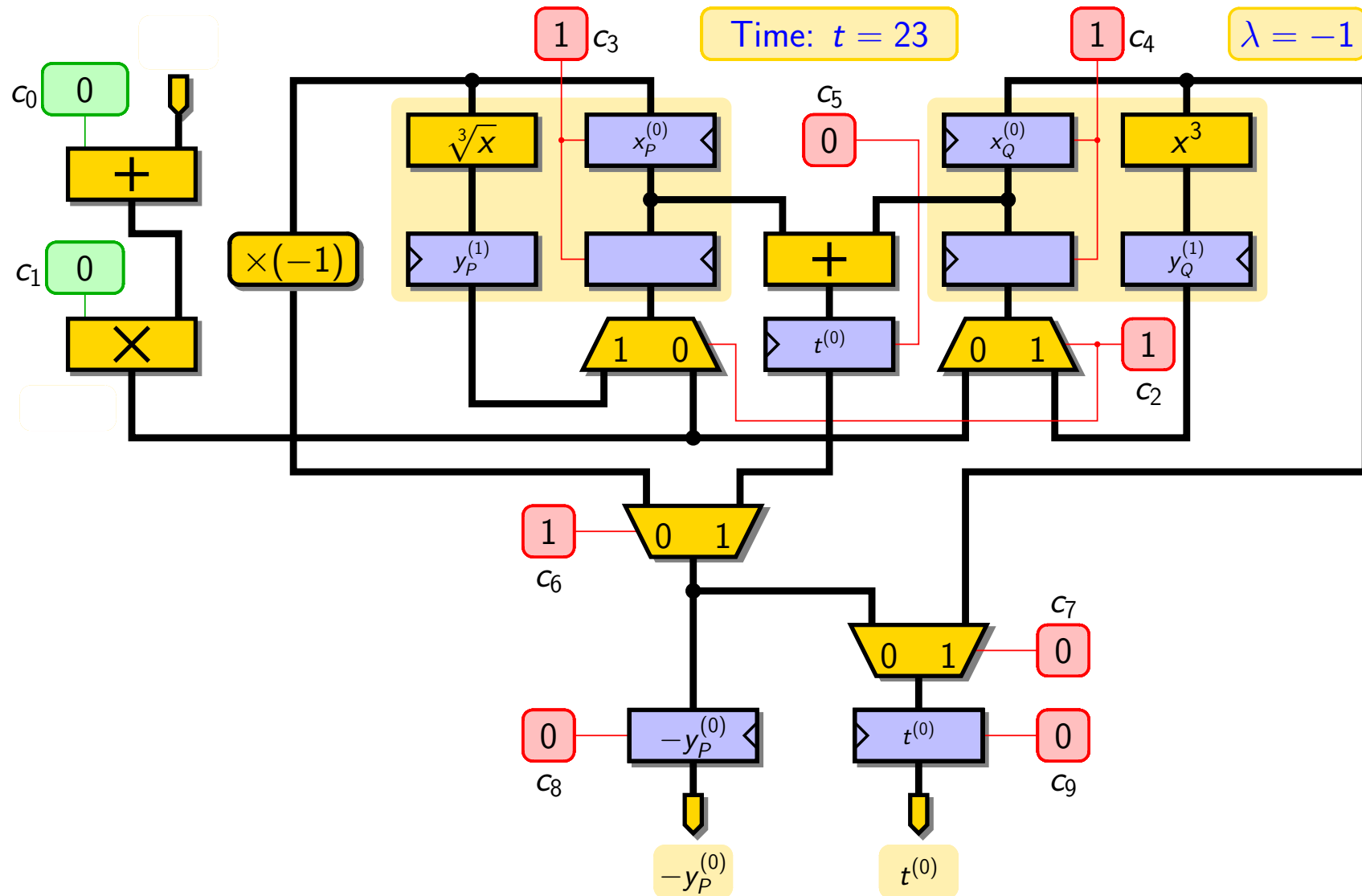


# Update of Coordinates of Points P and Q ( $\lambda = -1$ )

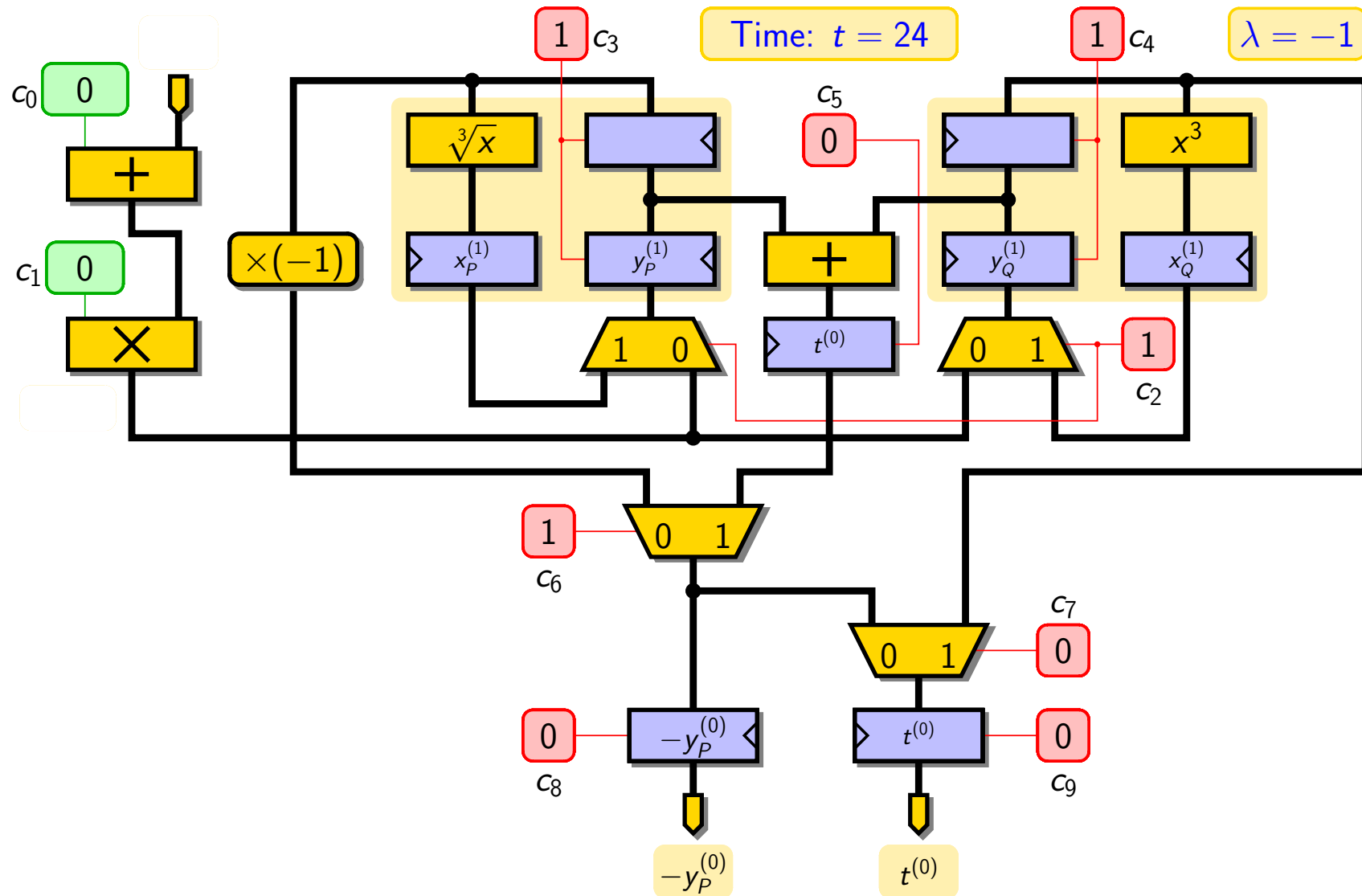




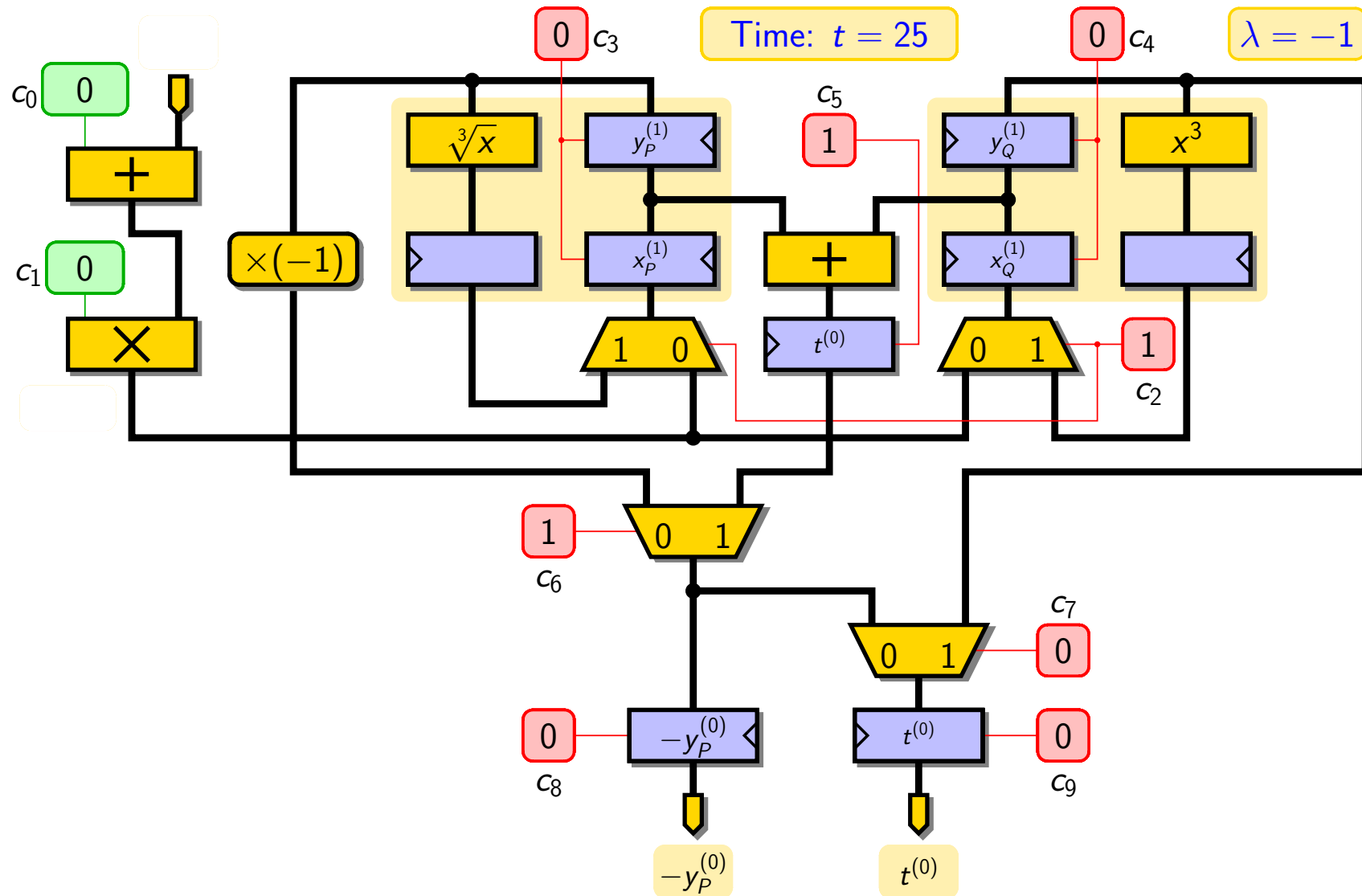
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



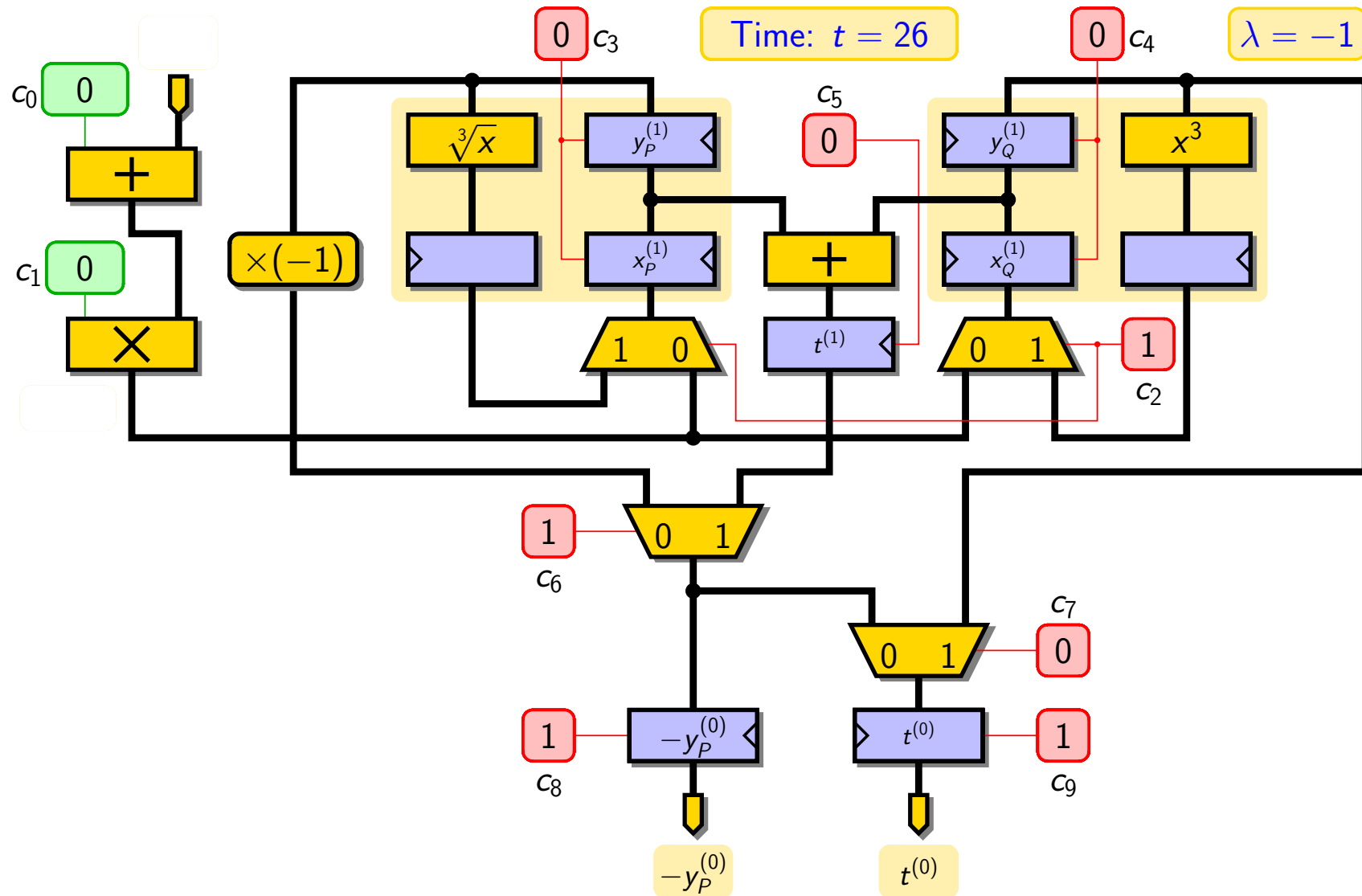
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



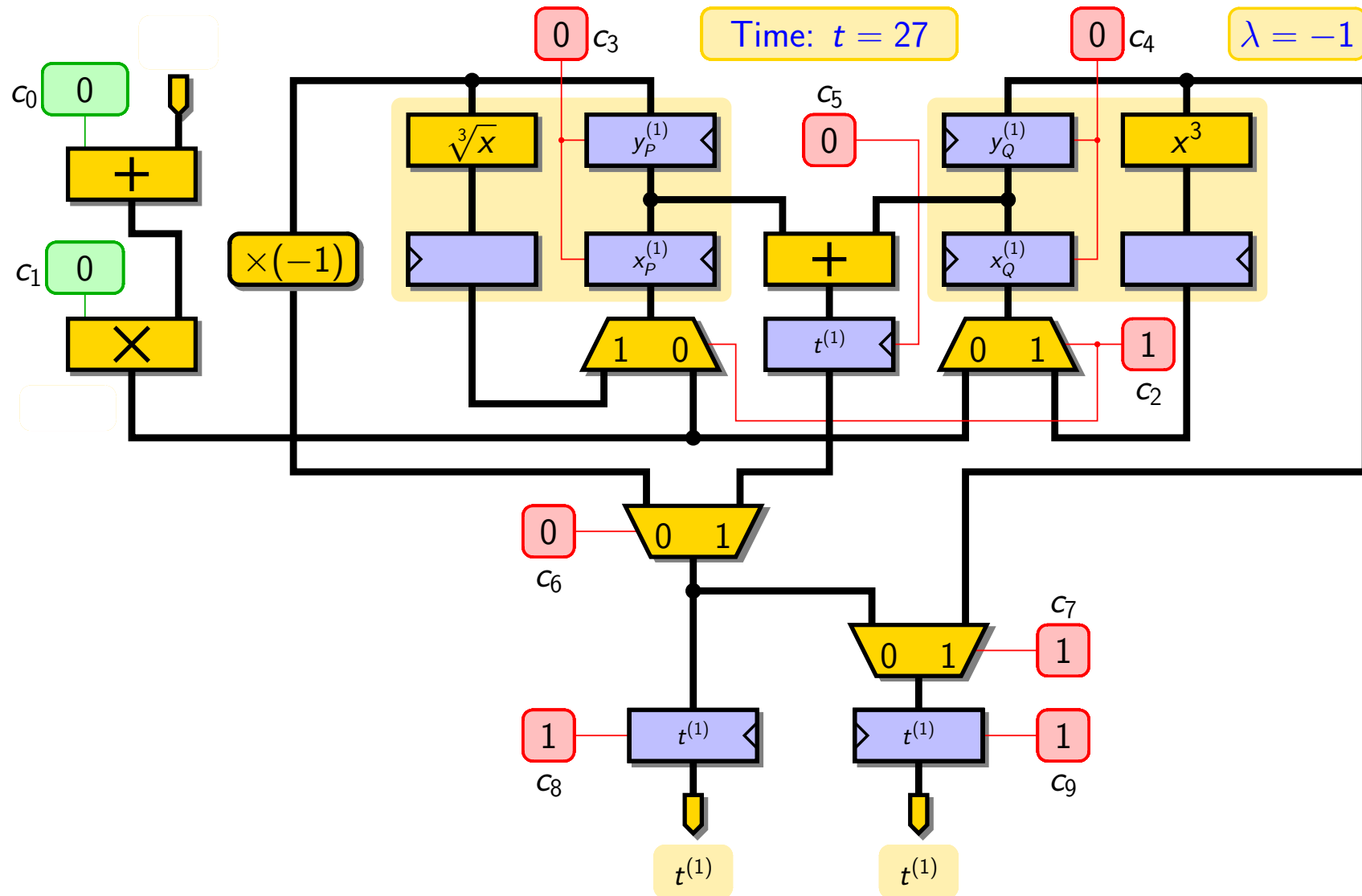
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



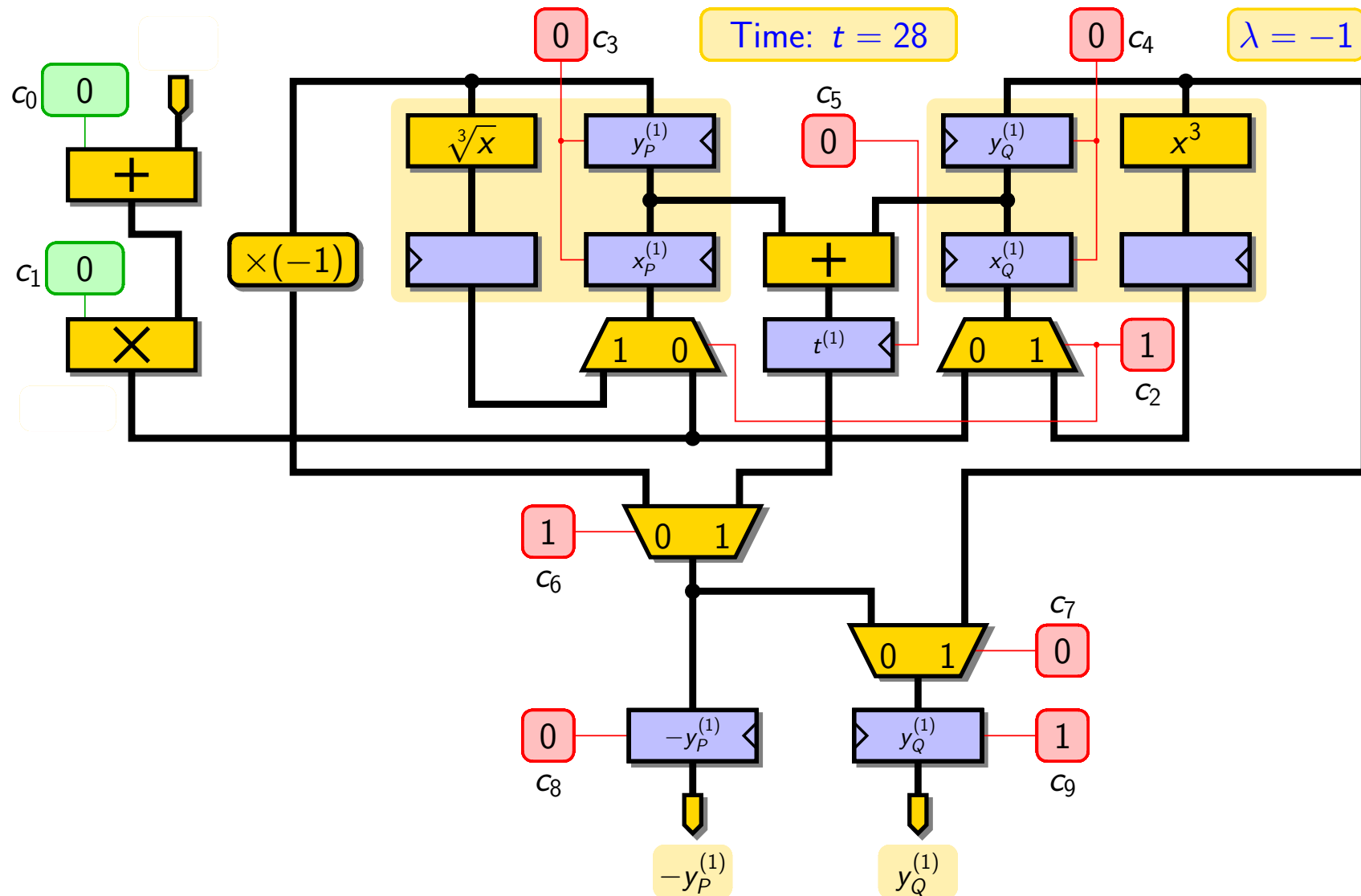
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



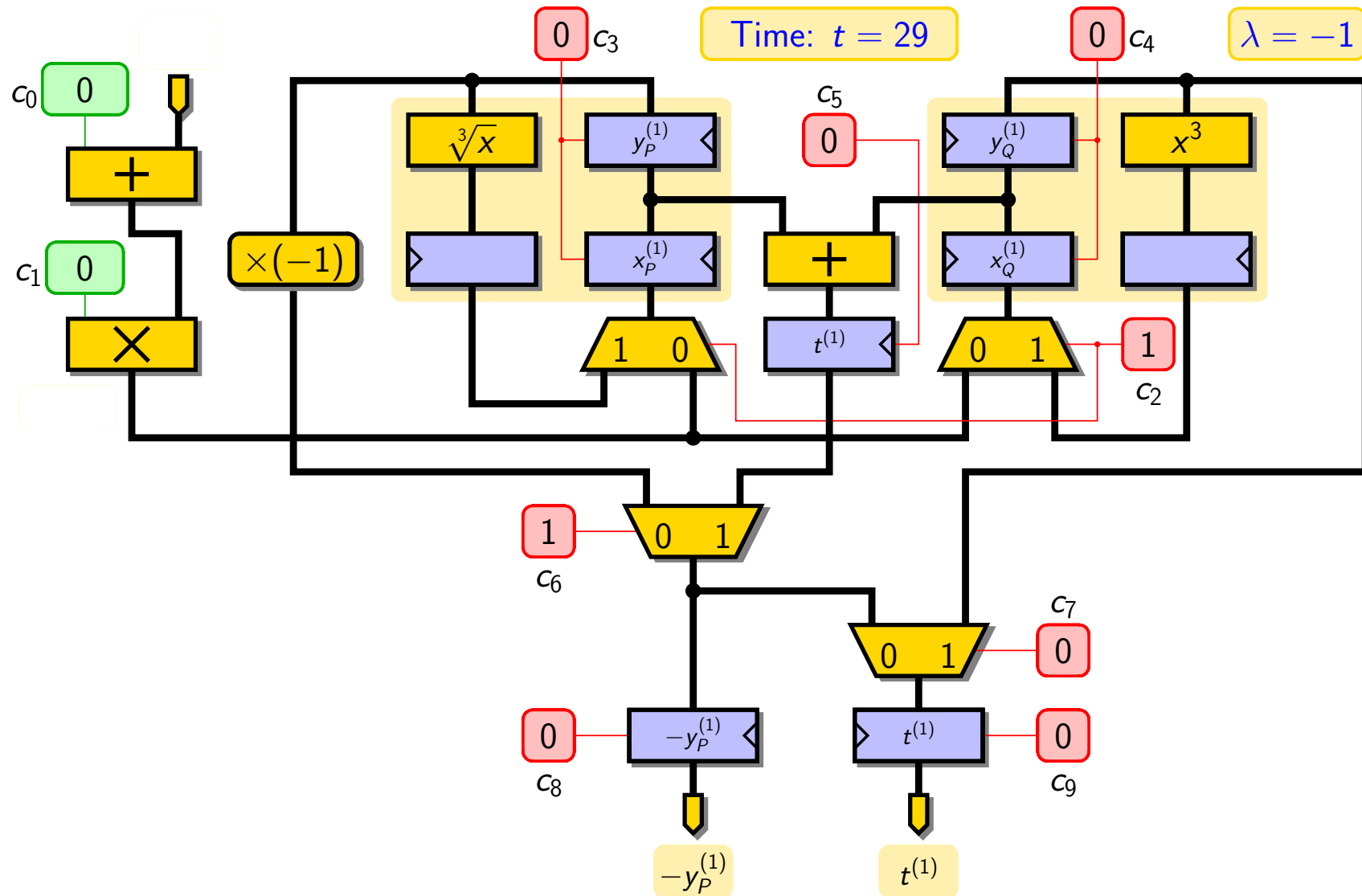
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



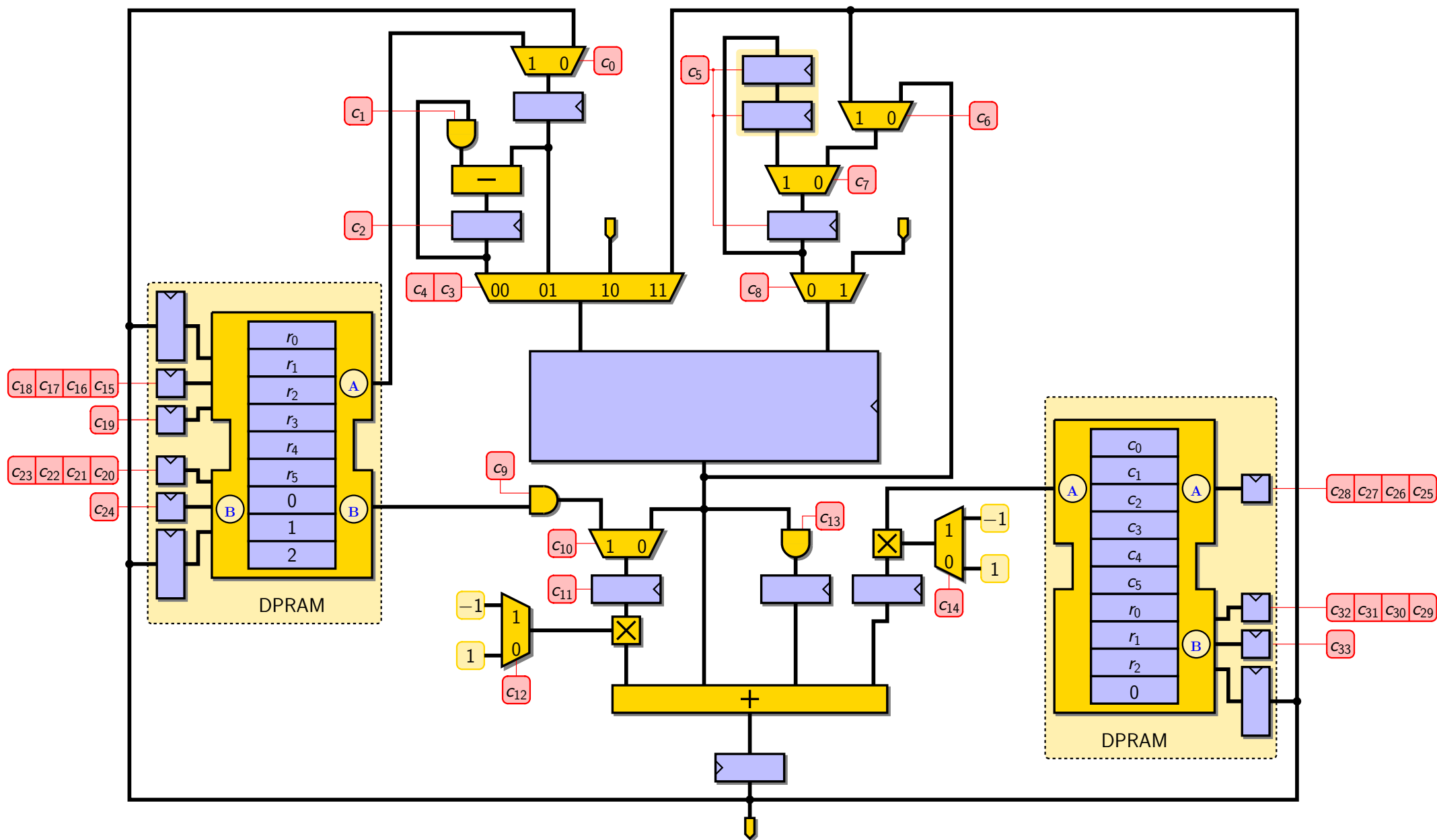
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



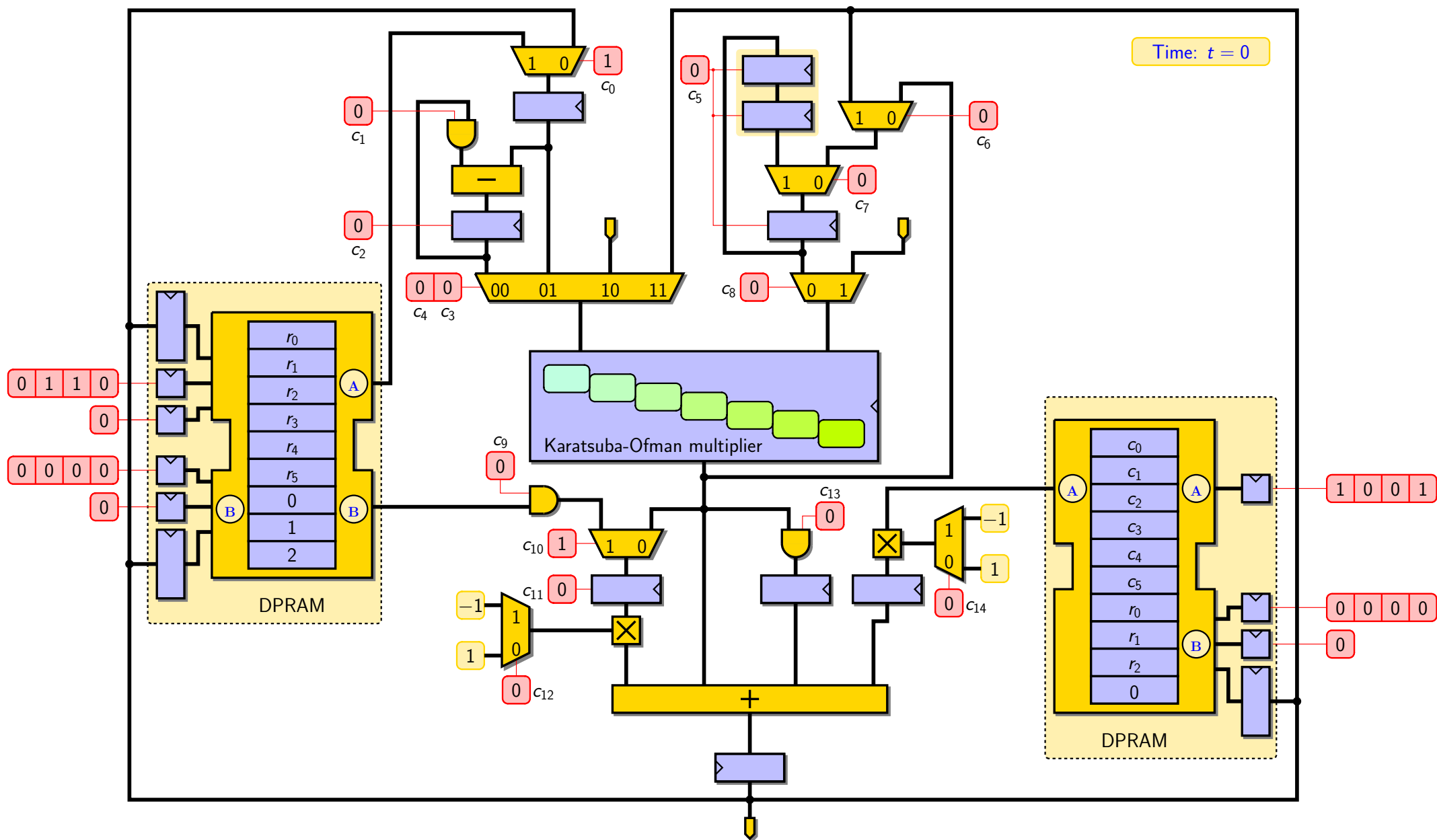
# Update of Coordinates of Points P and Q ( $\lambda = -1$ )



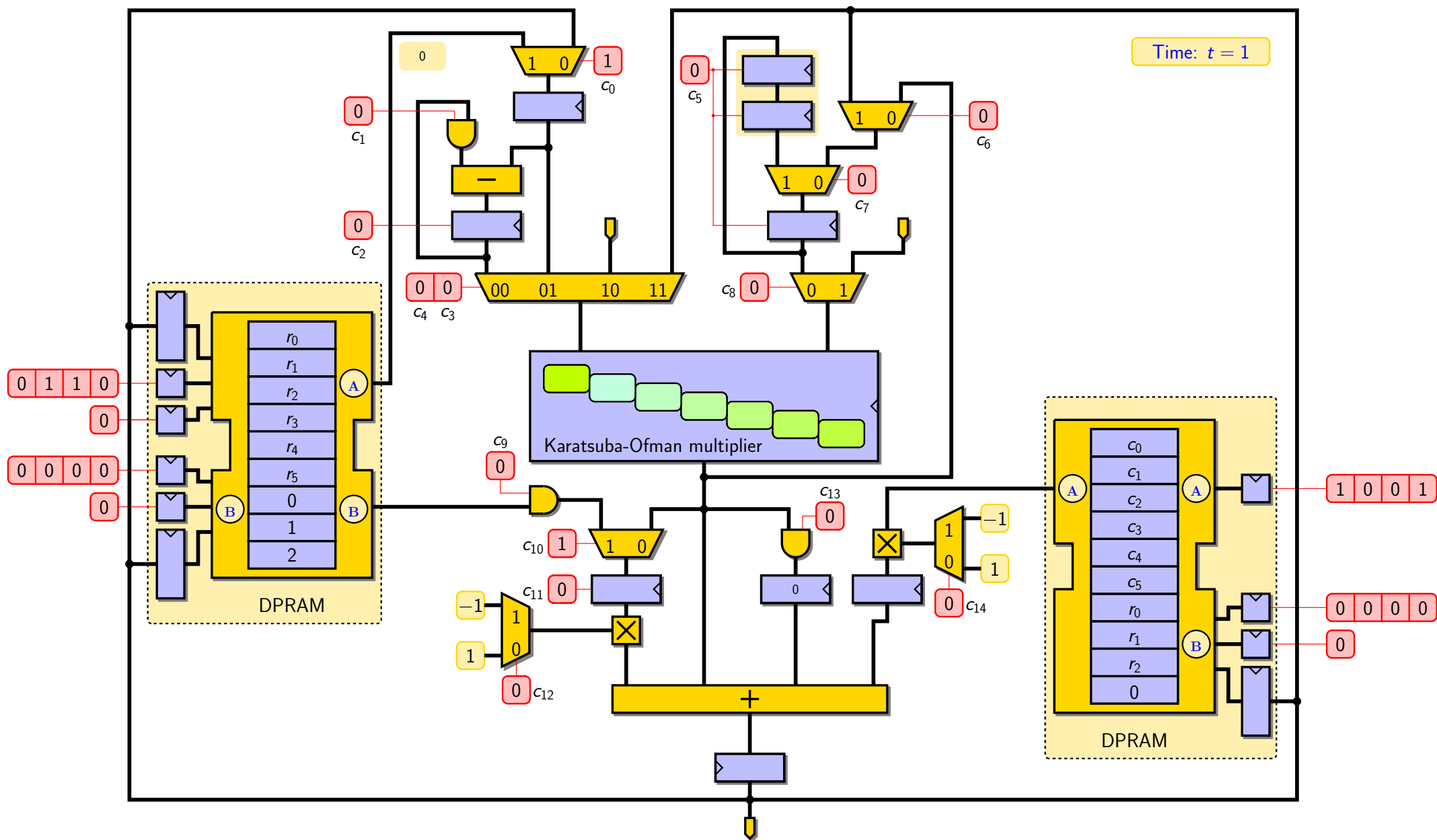
# Sparse Multiplication Over $\mathbb{F}_{36m}$



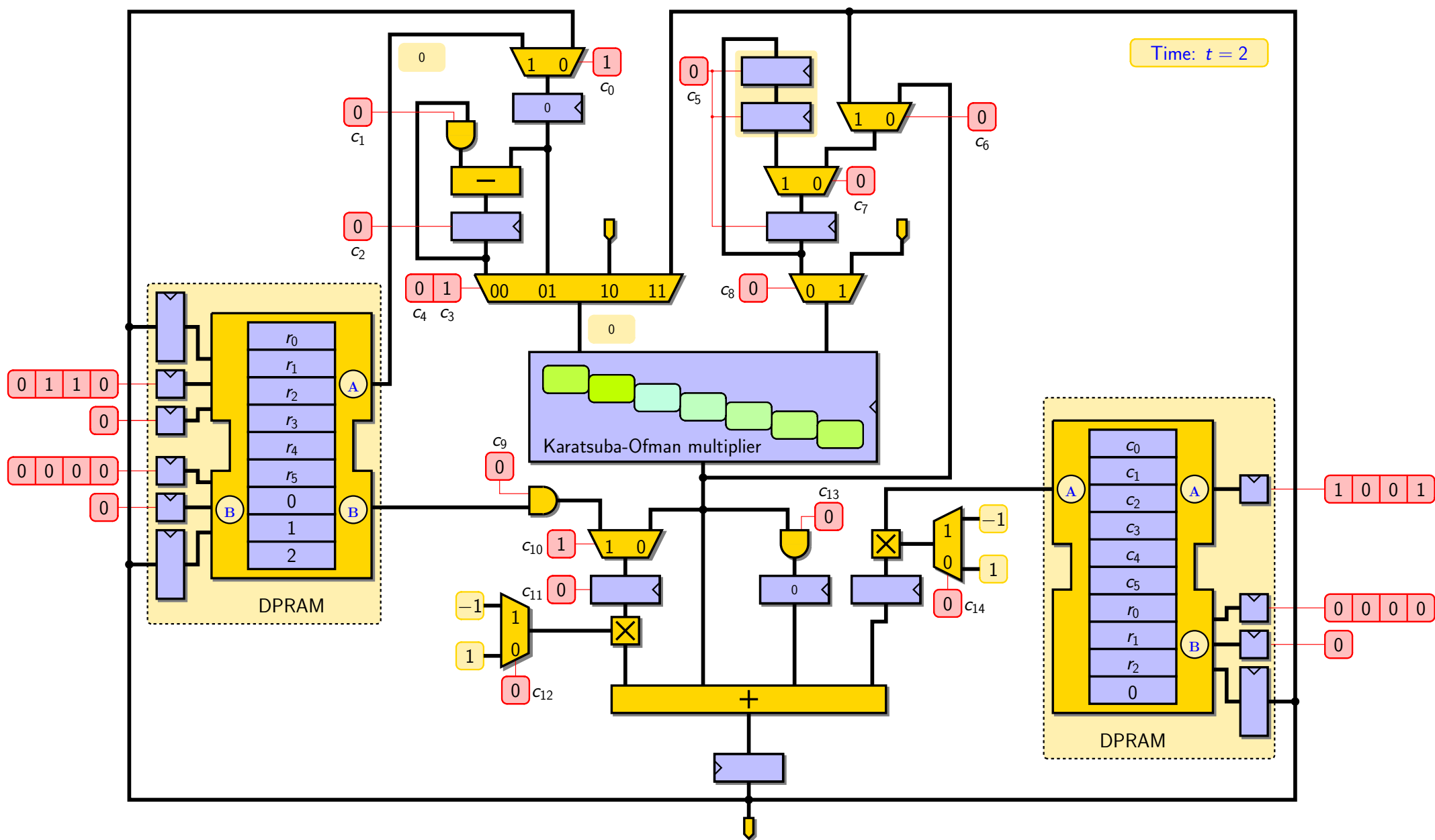
# Sparse Multiplication Over $\mathbb{F}_{36m}$



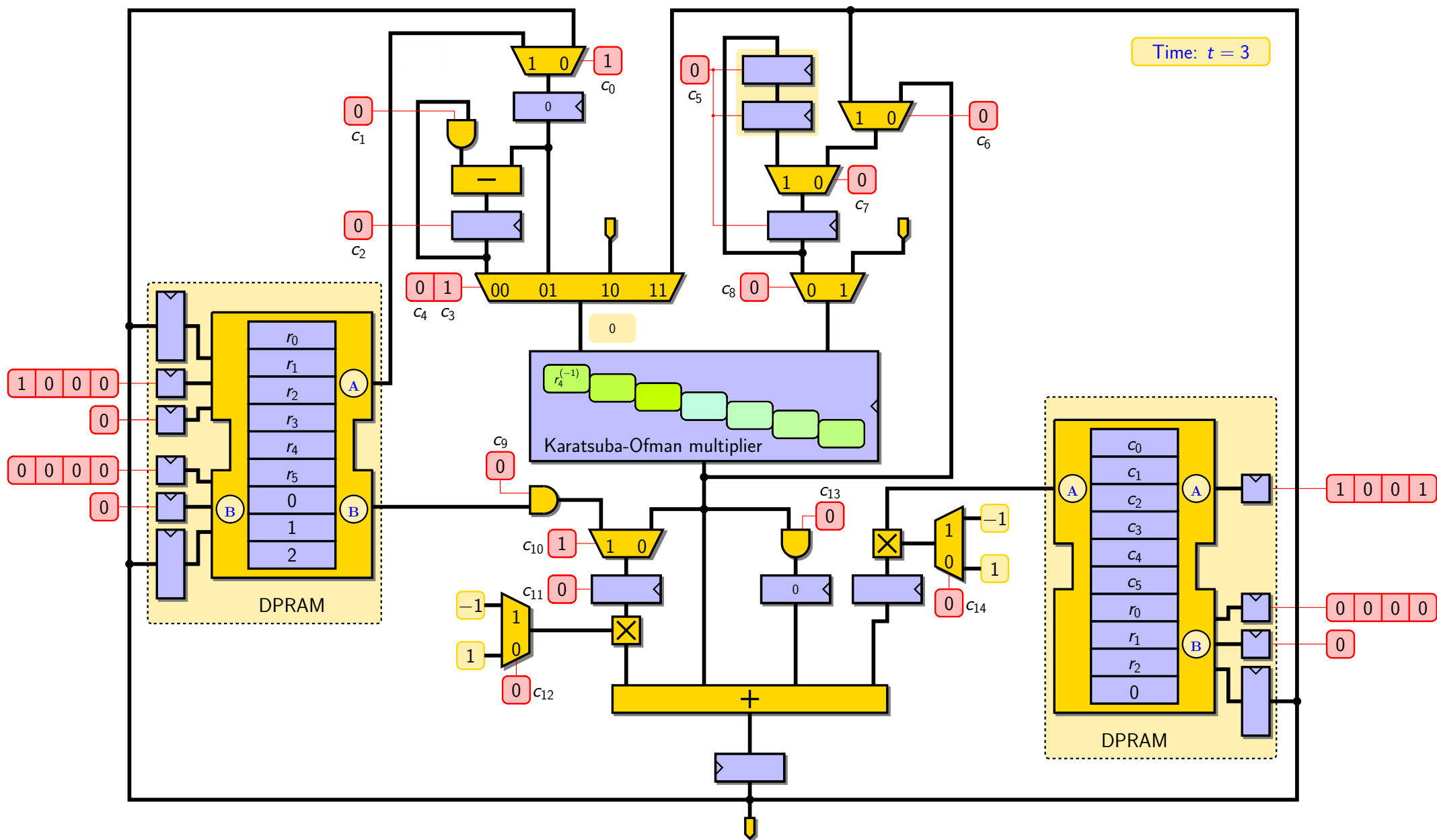
# Sparse Multiplication Over $\mathbb{F}_{36m}$



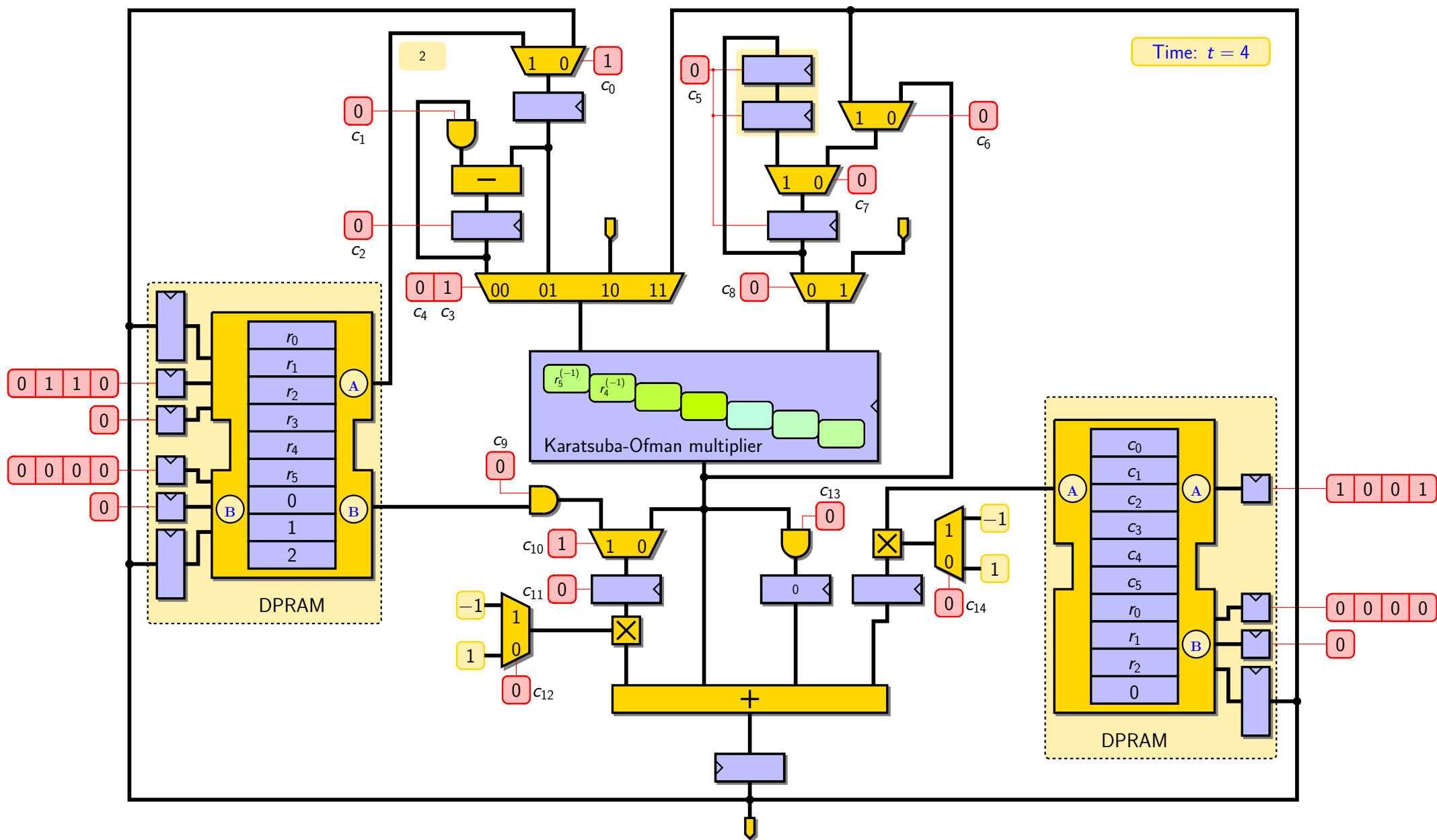
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



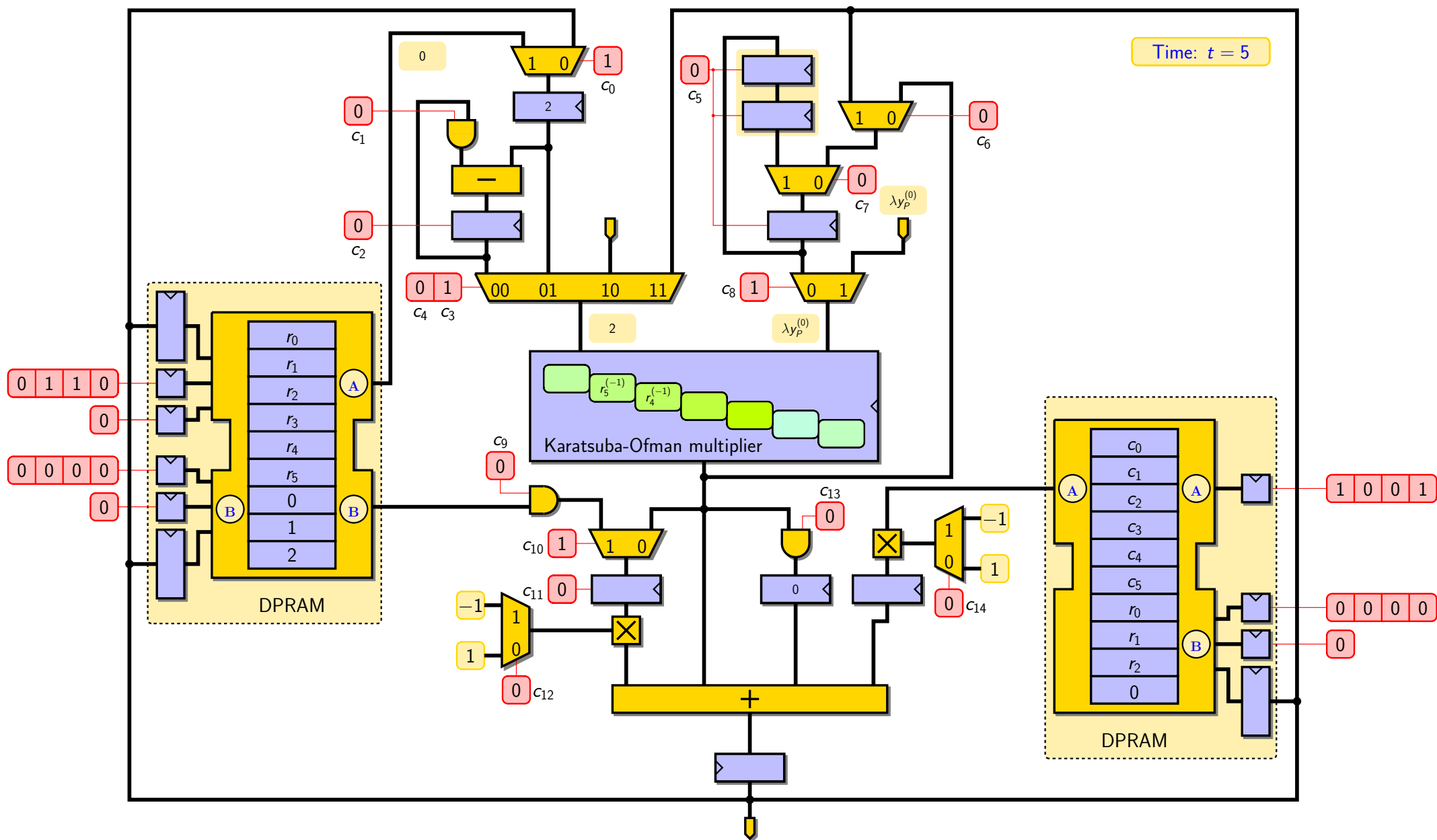
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



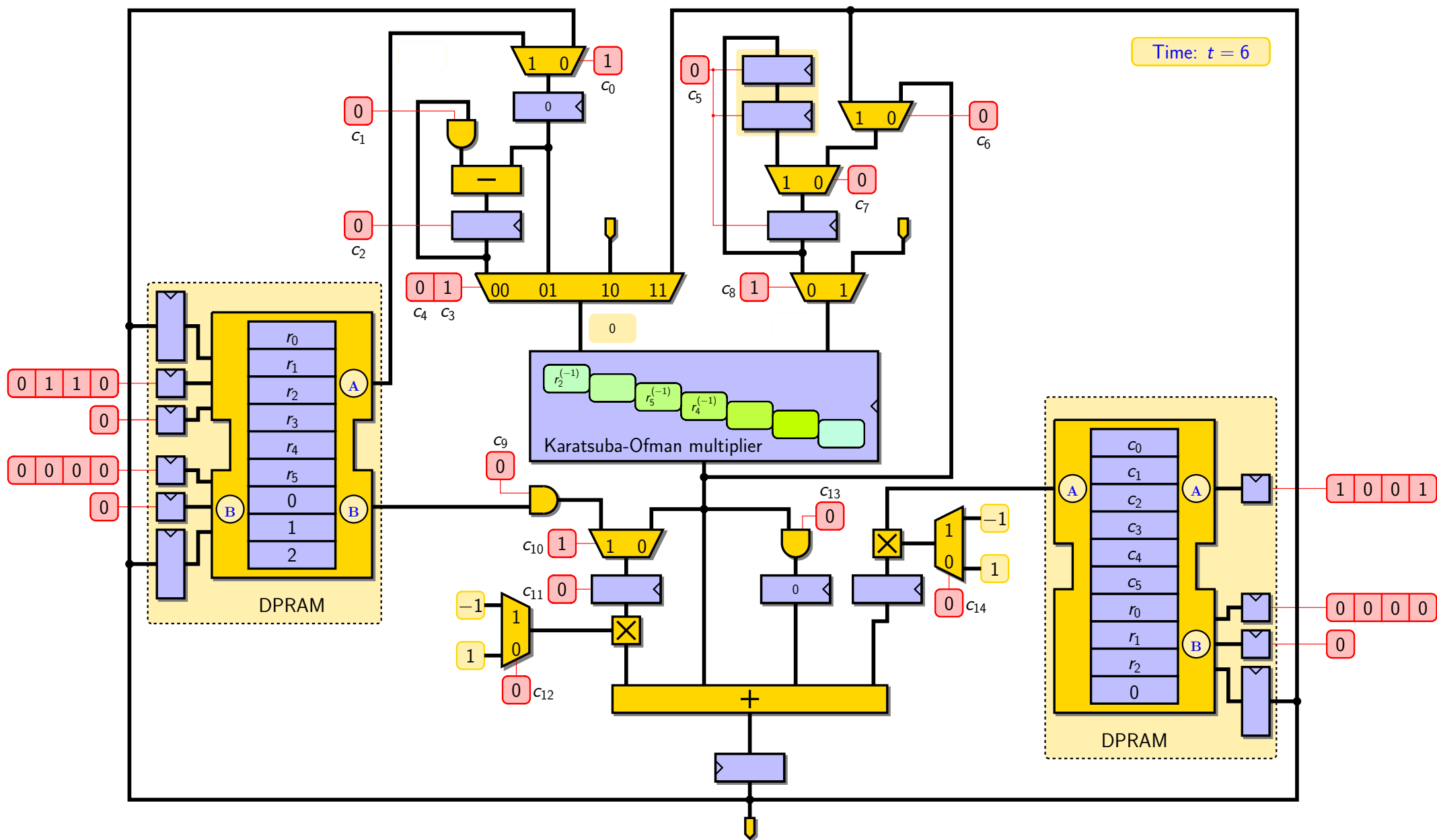
# Sparse Multiplication Over $\mathbb{F}_{36m}$



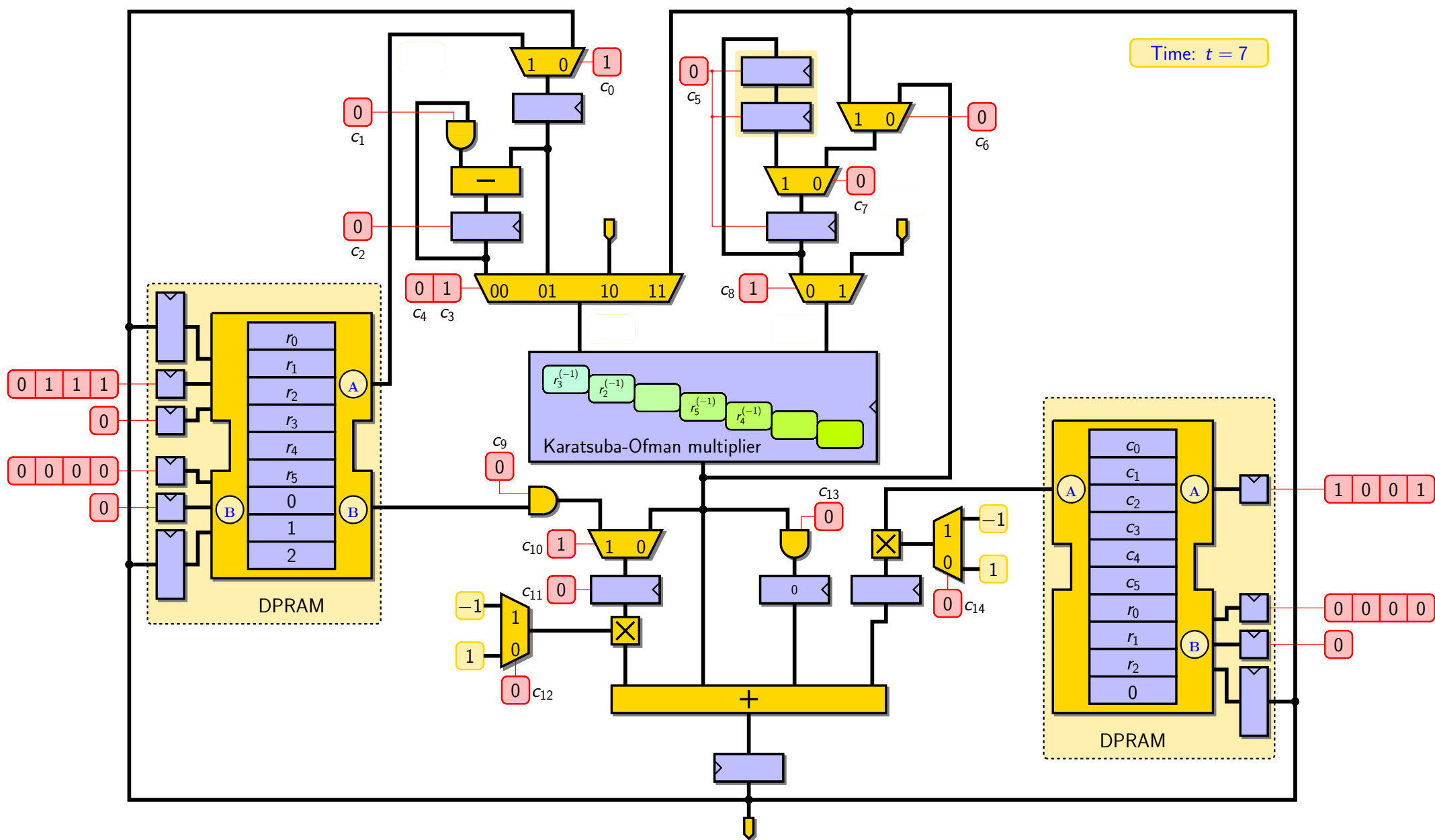
# Sparse Multiplication Over $\mathbb{F}_{36m}$



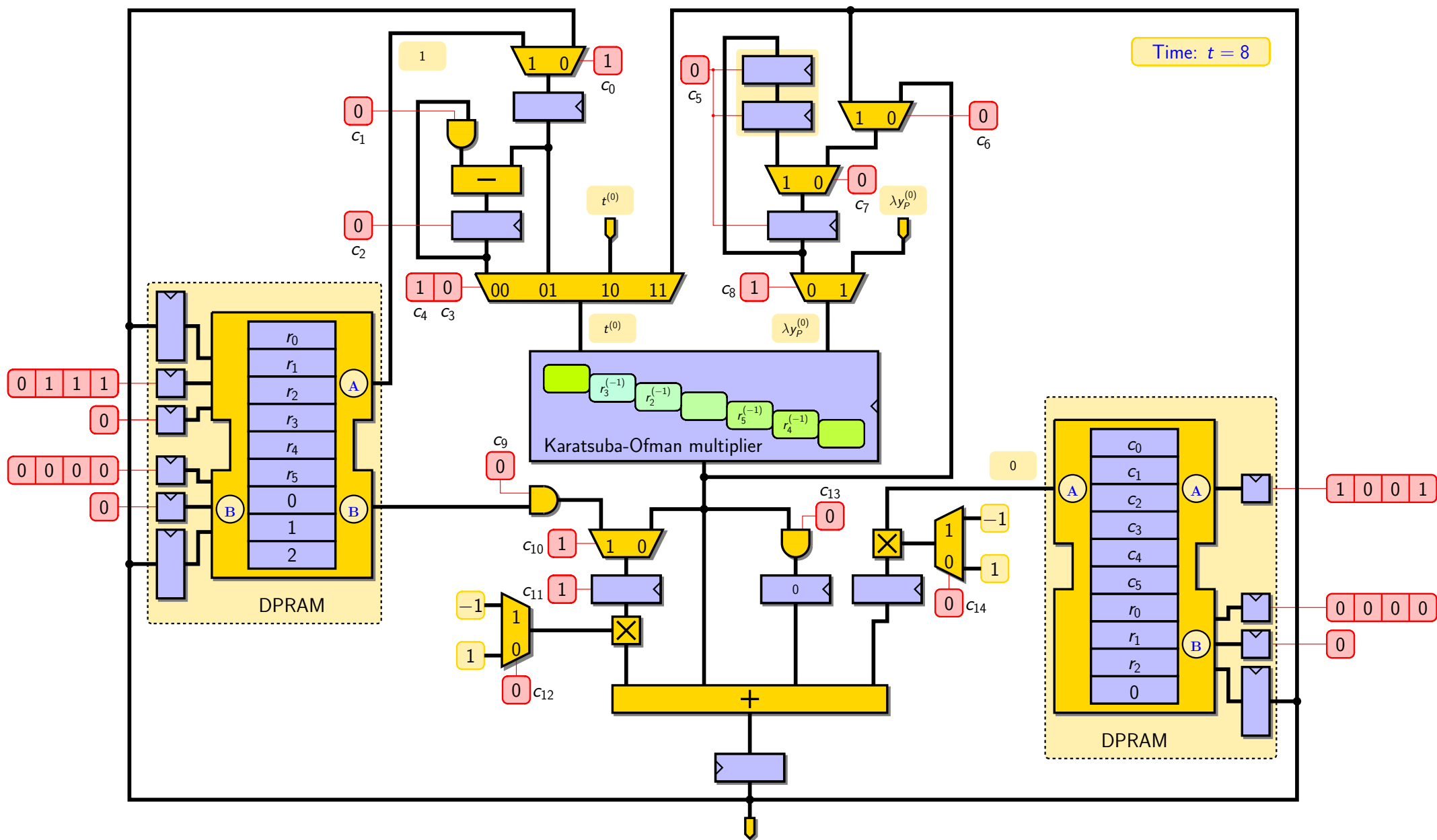
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



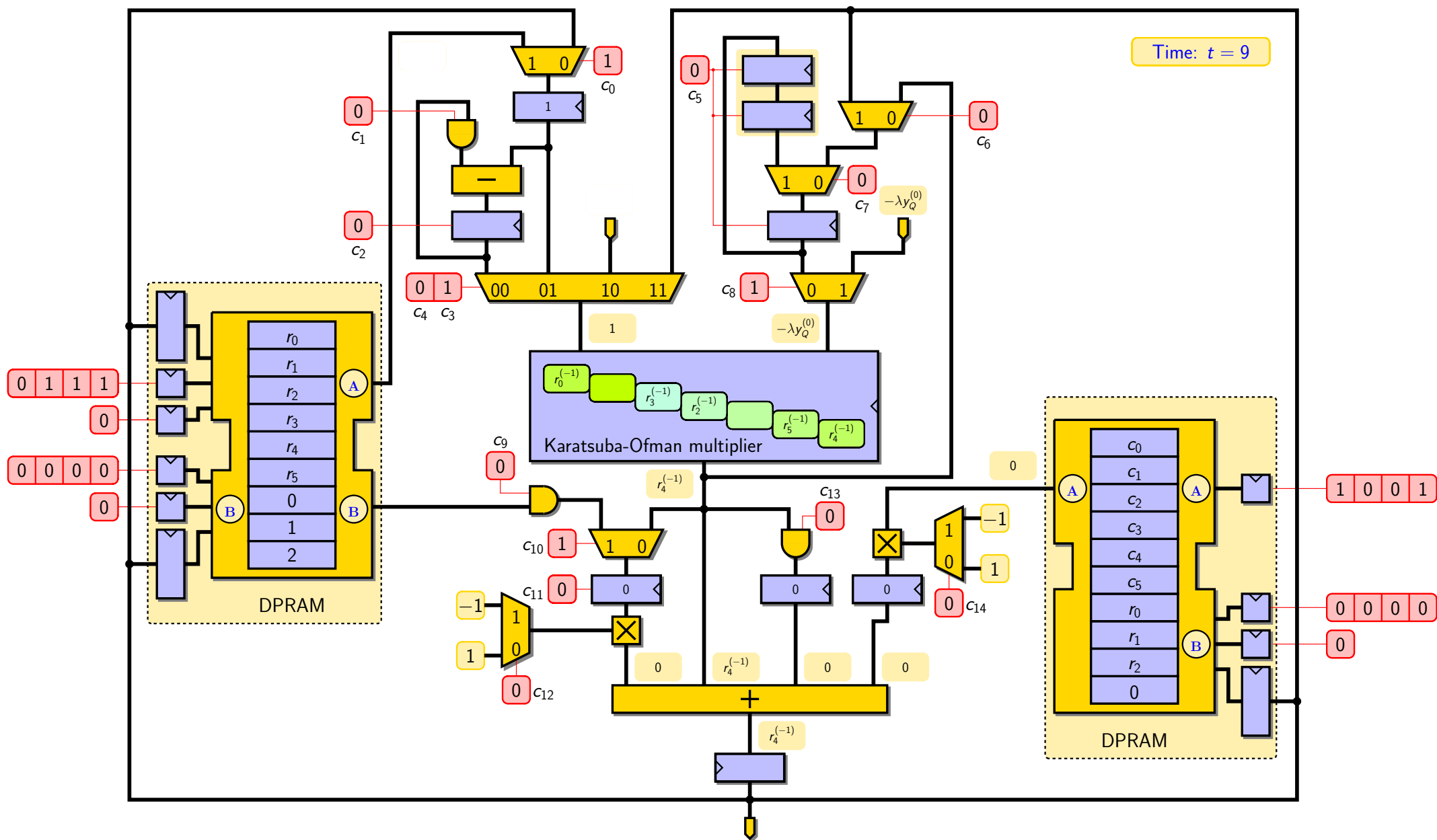
# Sparse Multiplication Over $\mathbb{F}_{36m}$



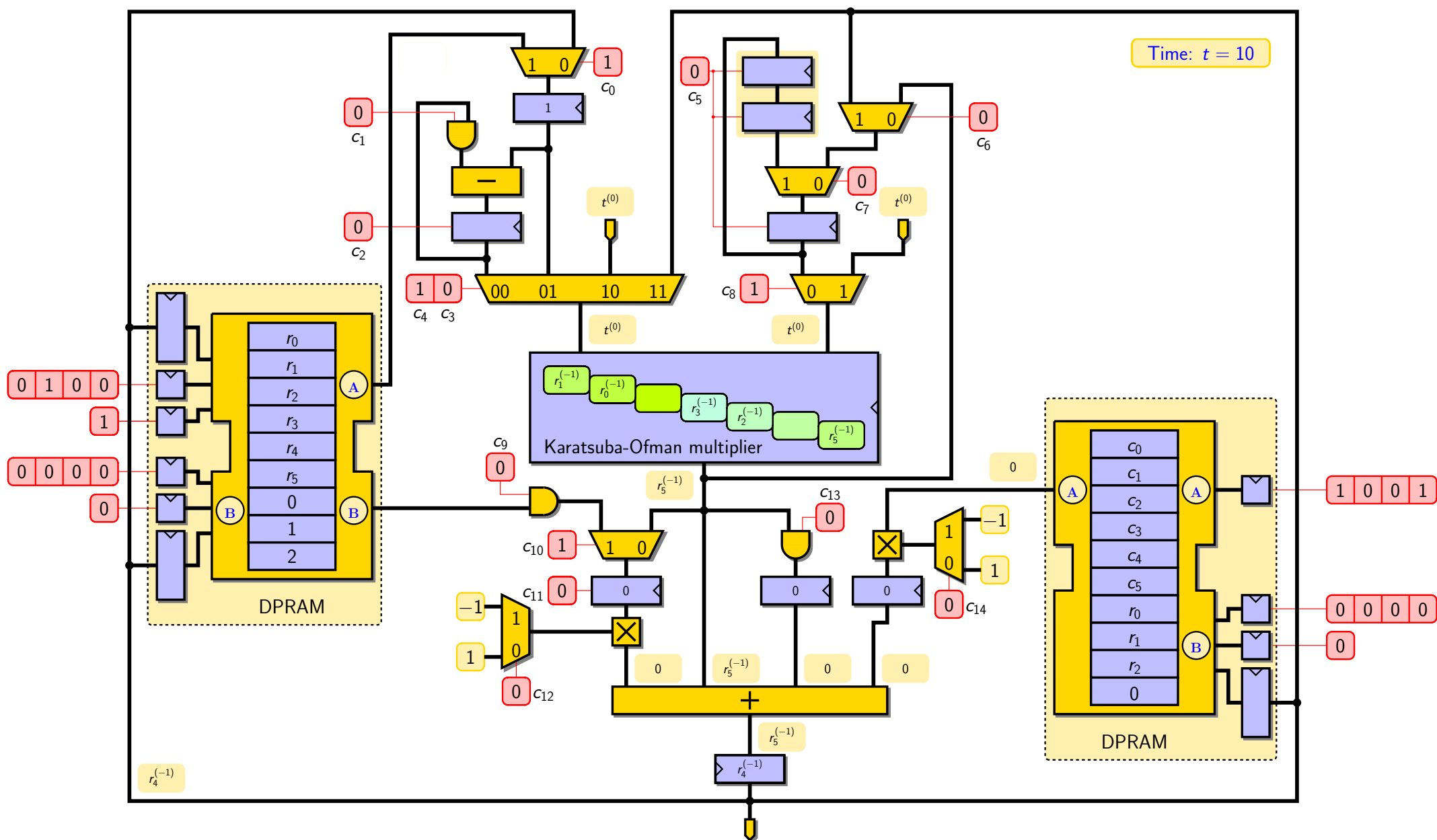
# Sparse Multiplication Over $\mathbb{F}_{36m}$



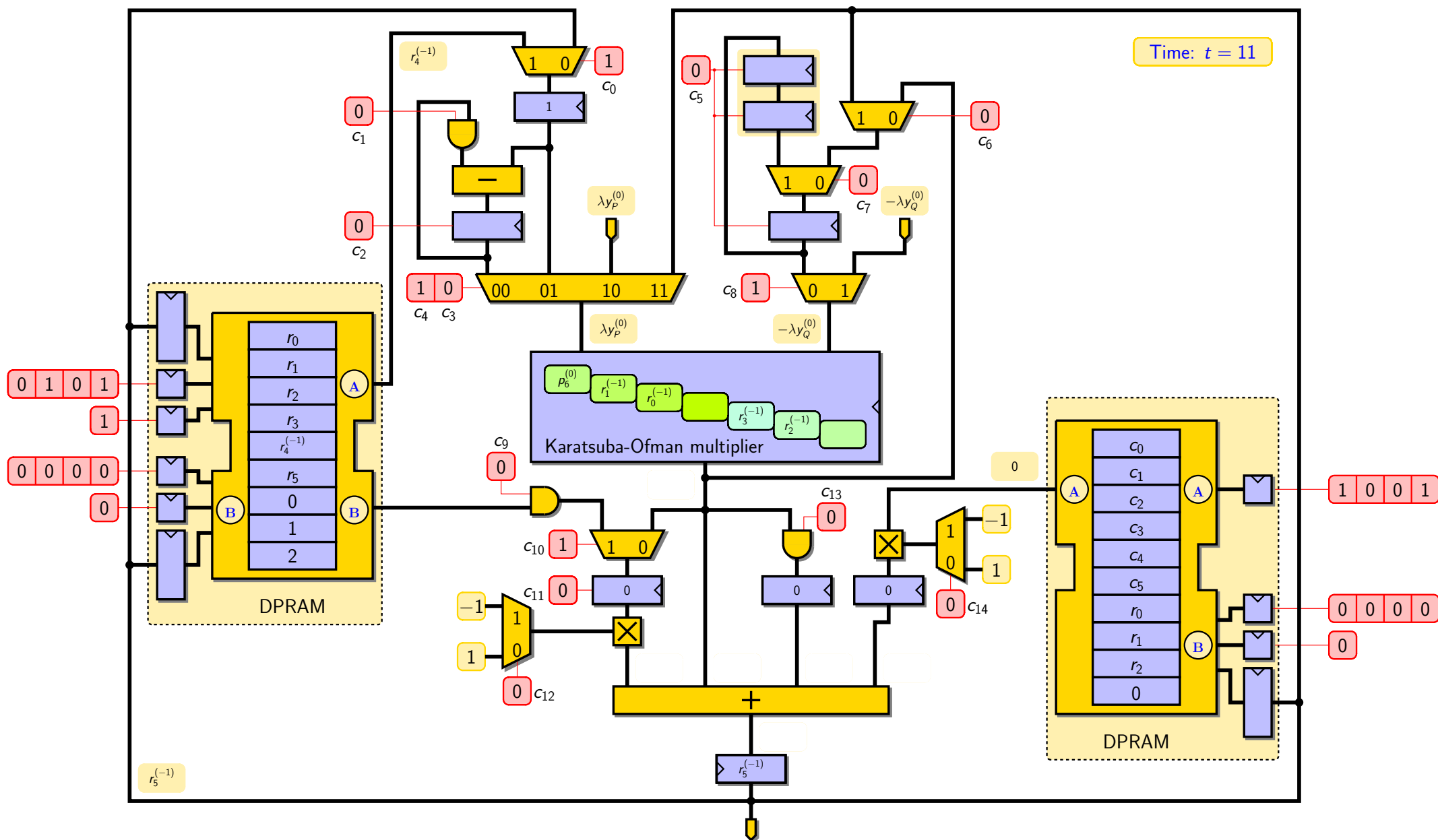
# Sparse Multiplication Over $\mathbb{F}_{36m}$



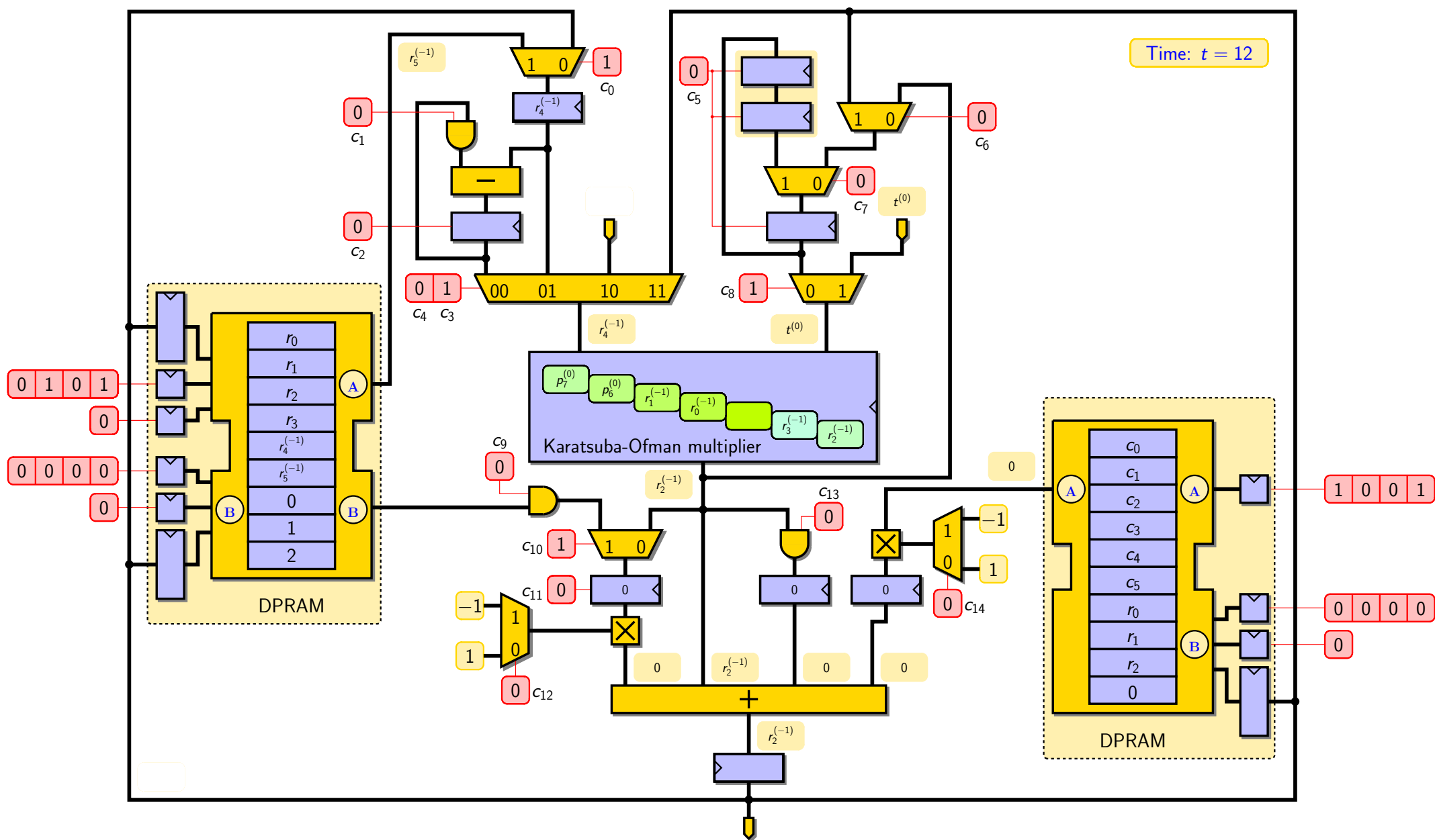
# Sparse Multiplication Over $\mathbb{F}_{36m}$



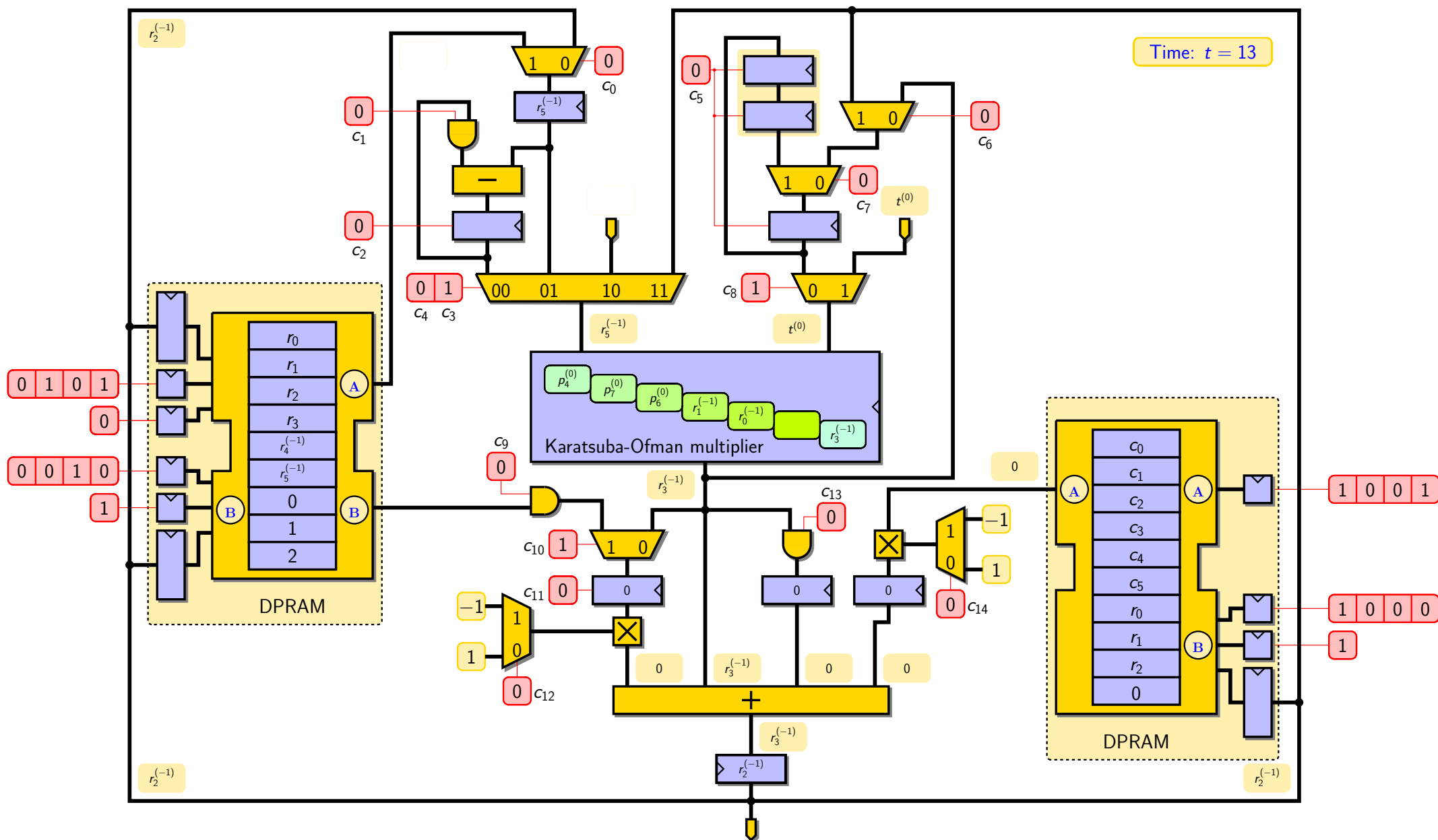
# Sparse Multiplication Over $\mathbb{F}_{36m}$



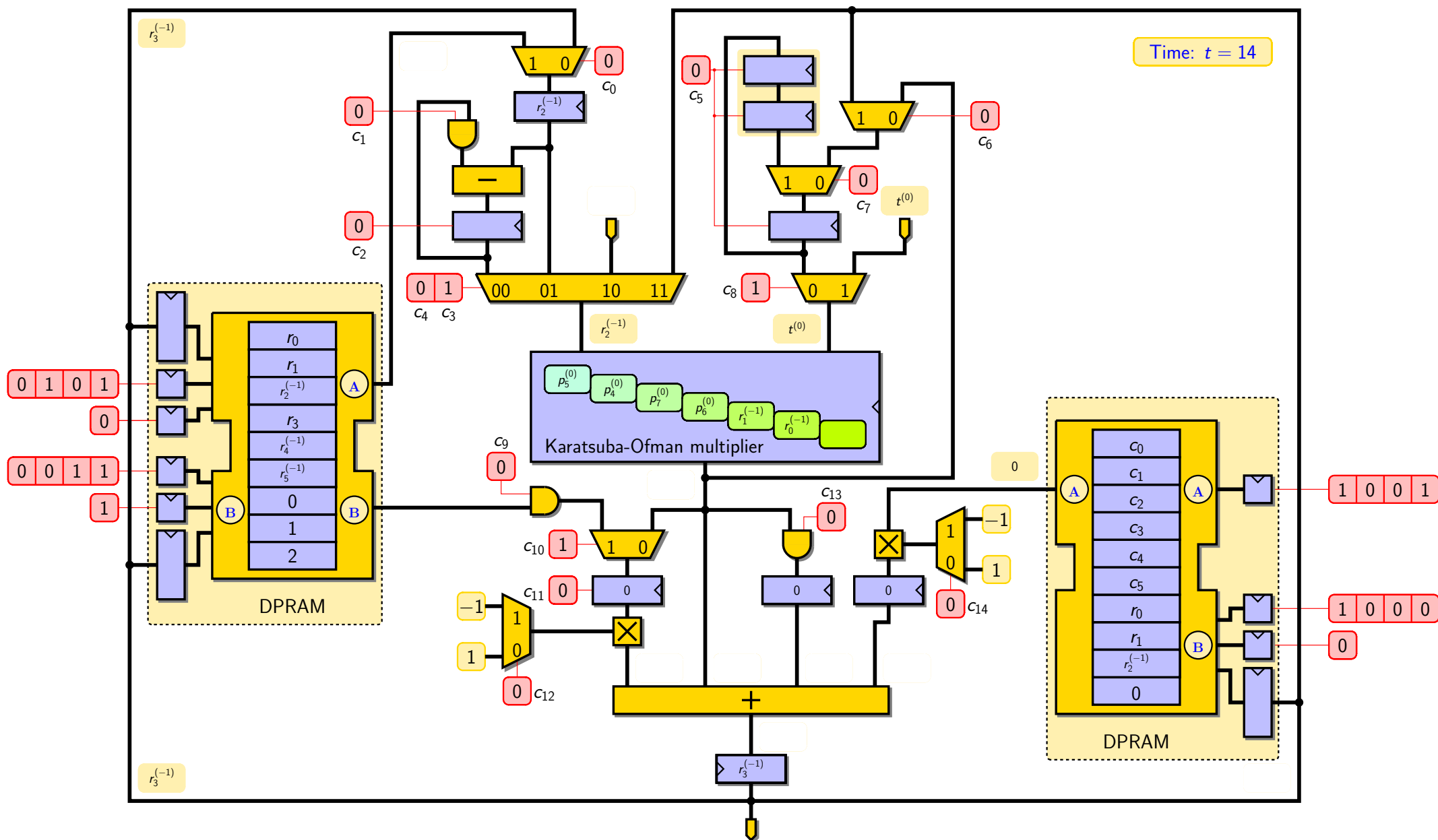
# Sparse Multiplication Over $\mathbb{F}_{36m}$



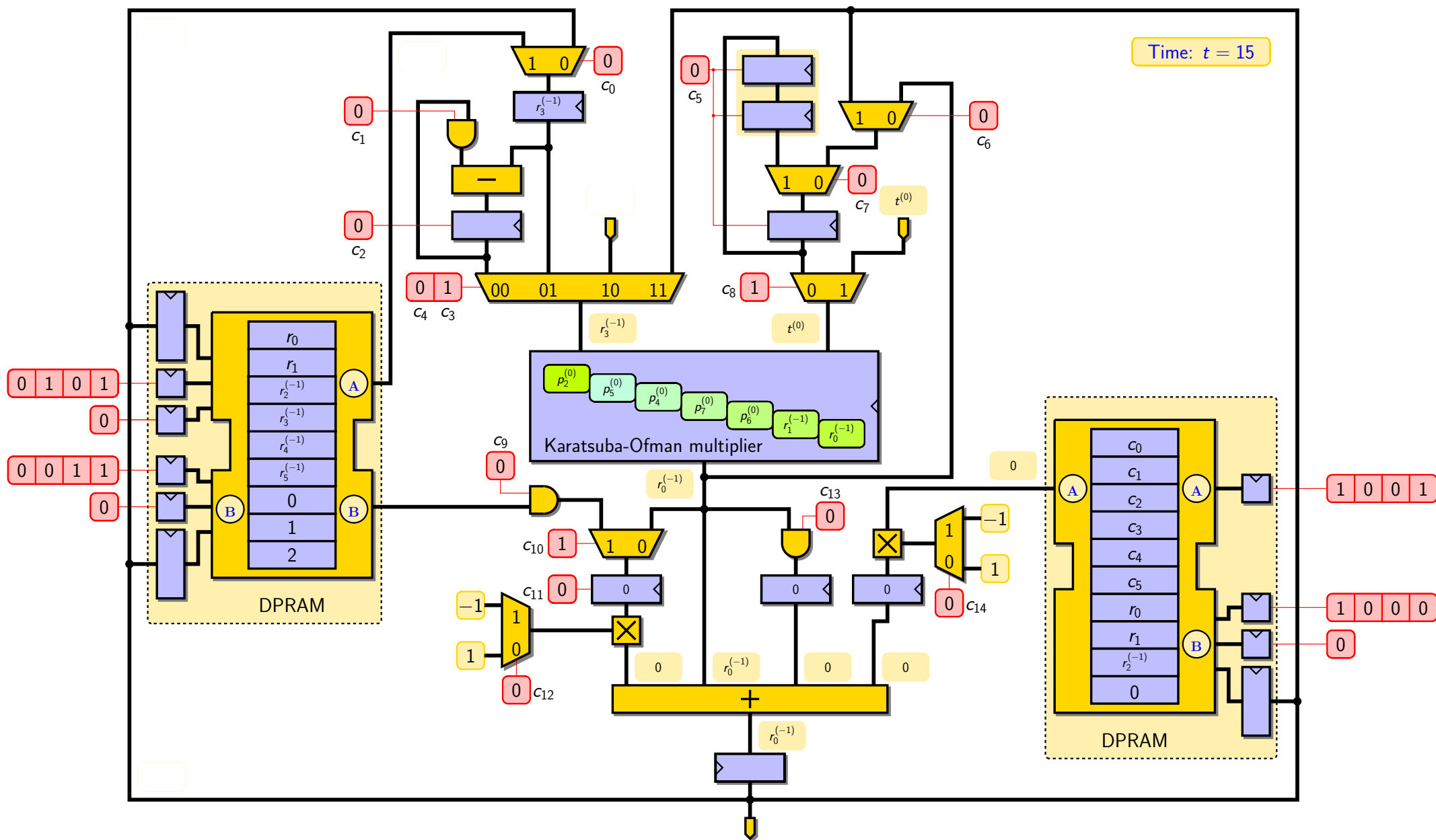
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



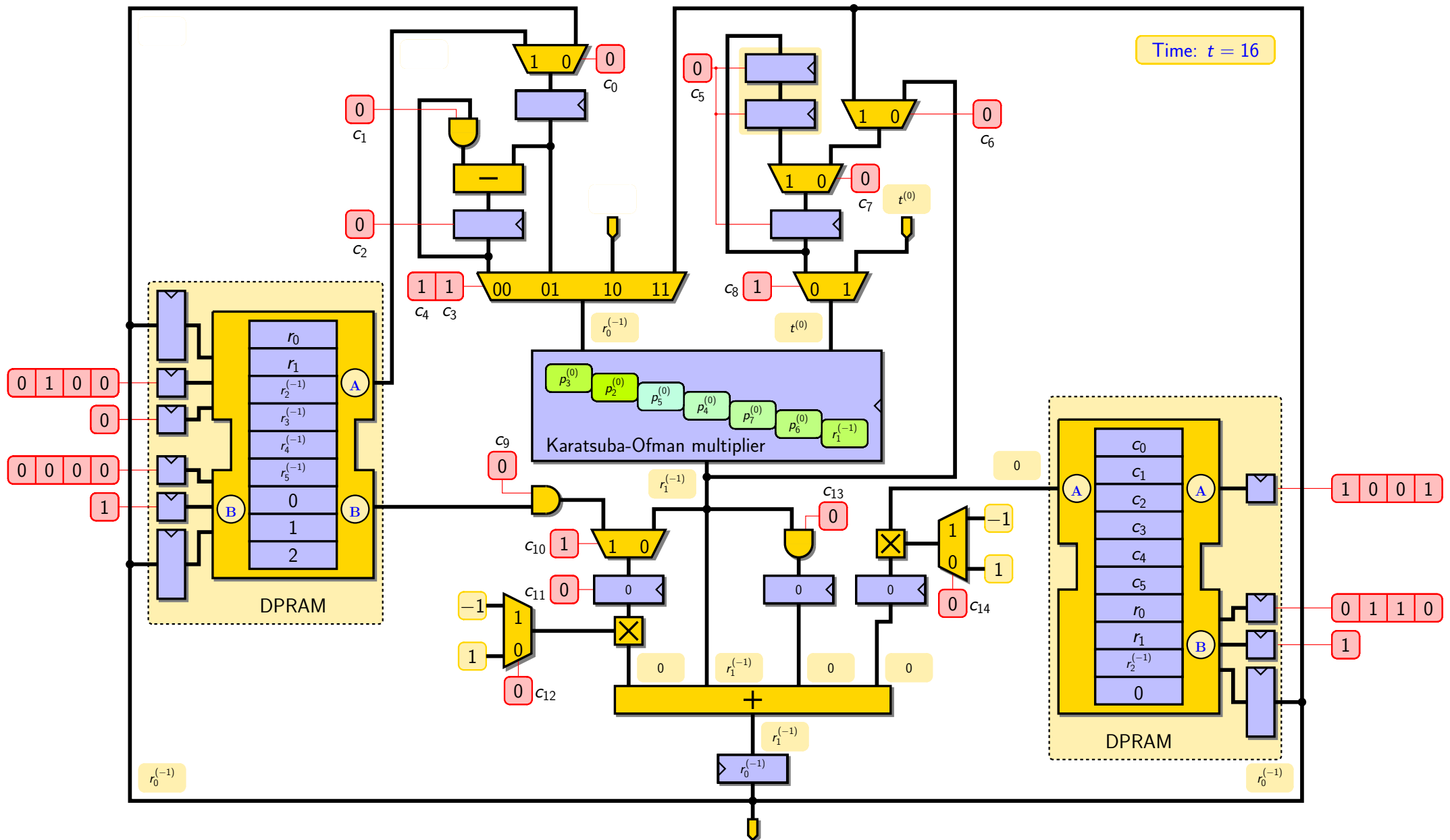
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



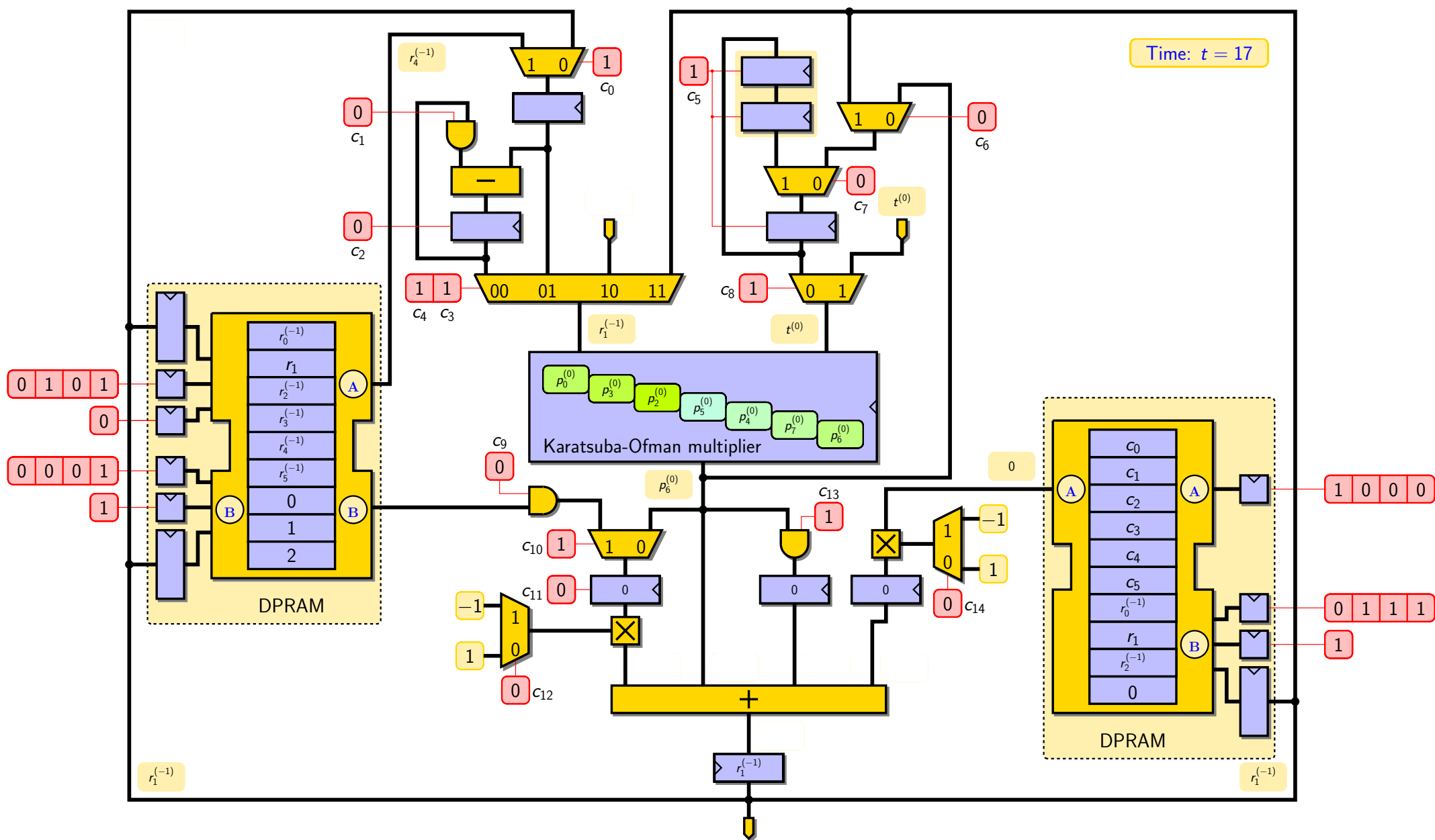
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



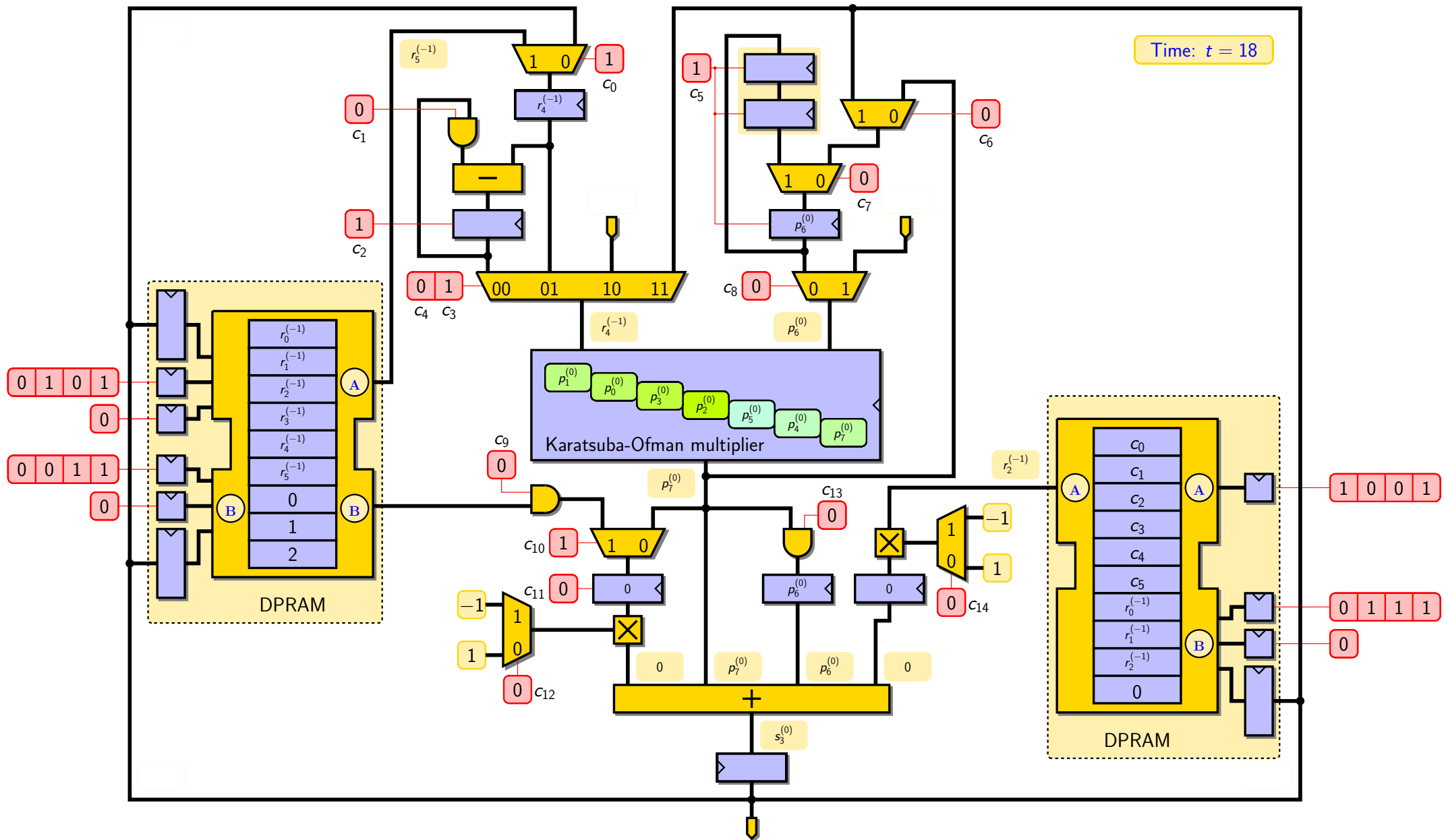
# Sparse Multiplication Over $\mathbb{F}_{36m}$



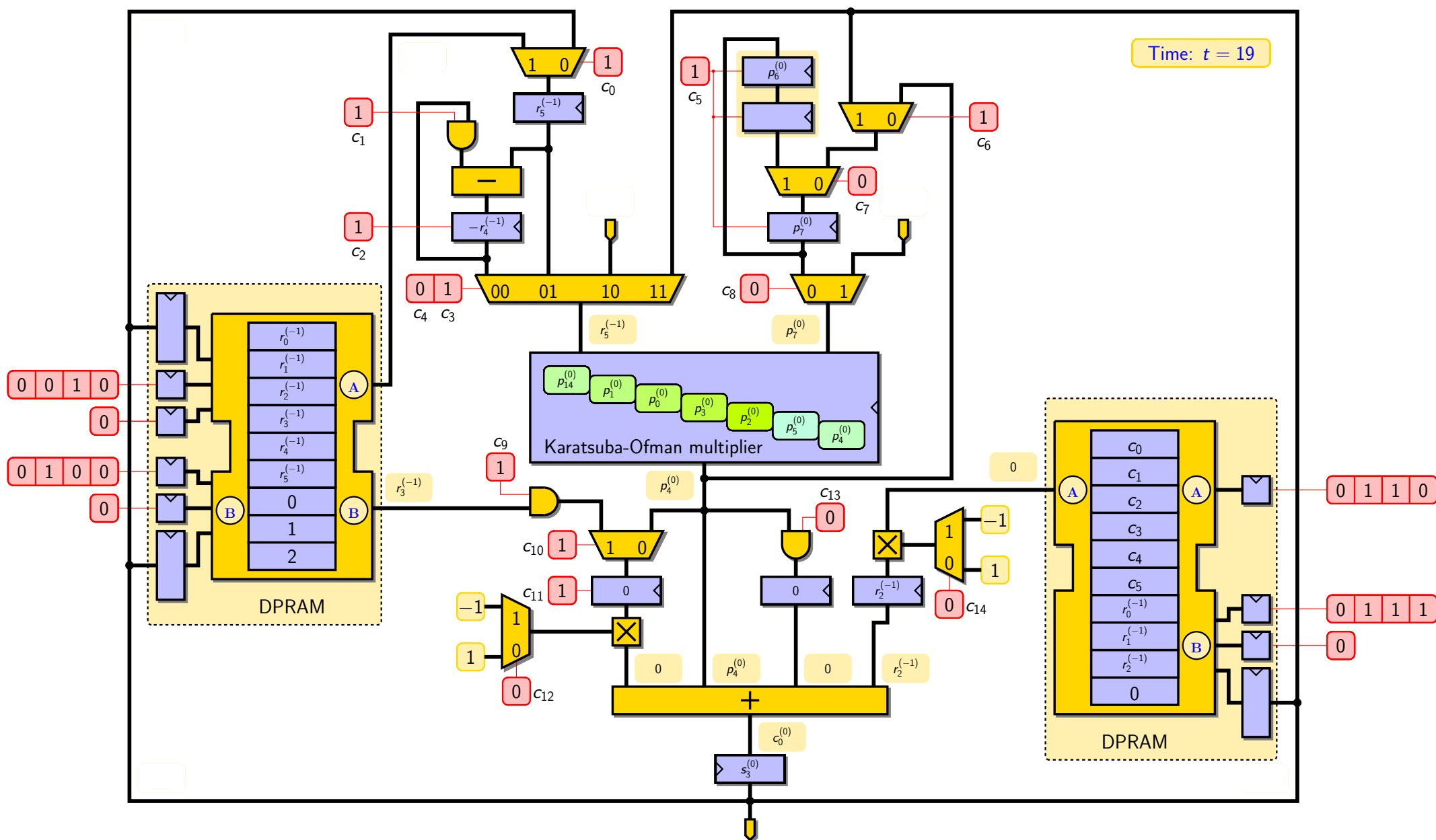
# Sparse Multiplication Over $\mathbb{F}_{36m}$



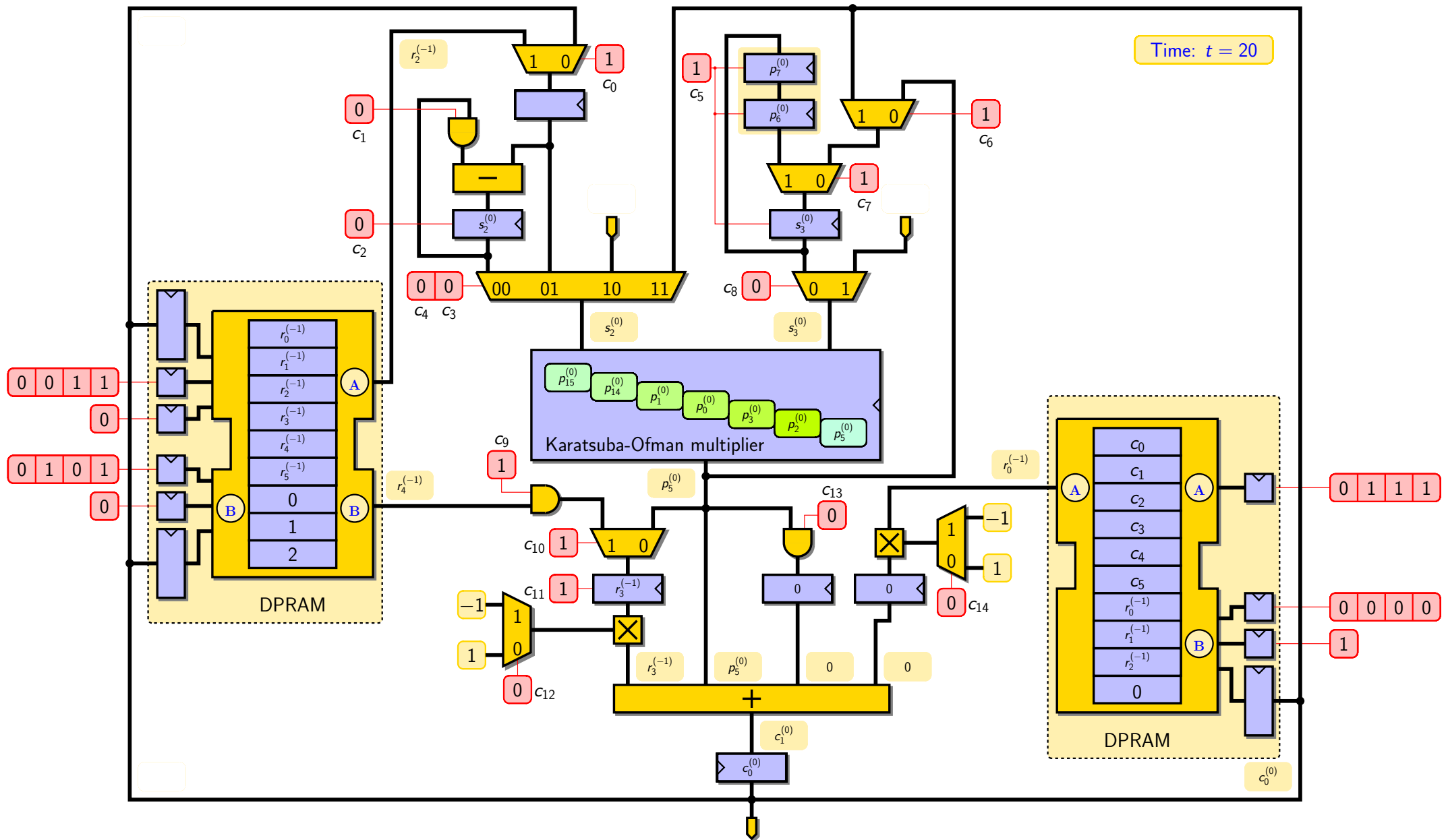
# Sparse Multiplication Over $\mathbb{F}_{36m}$



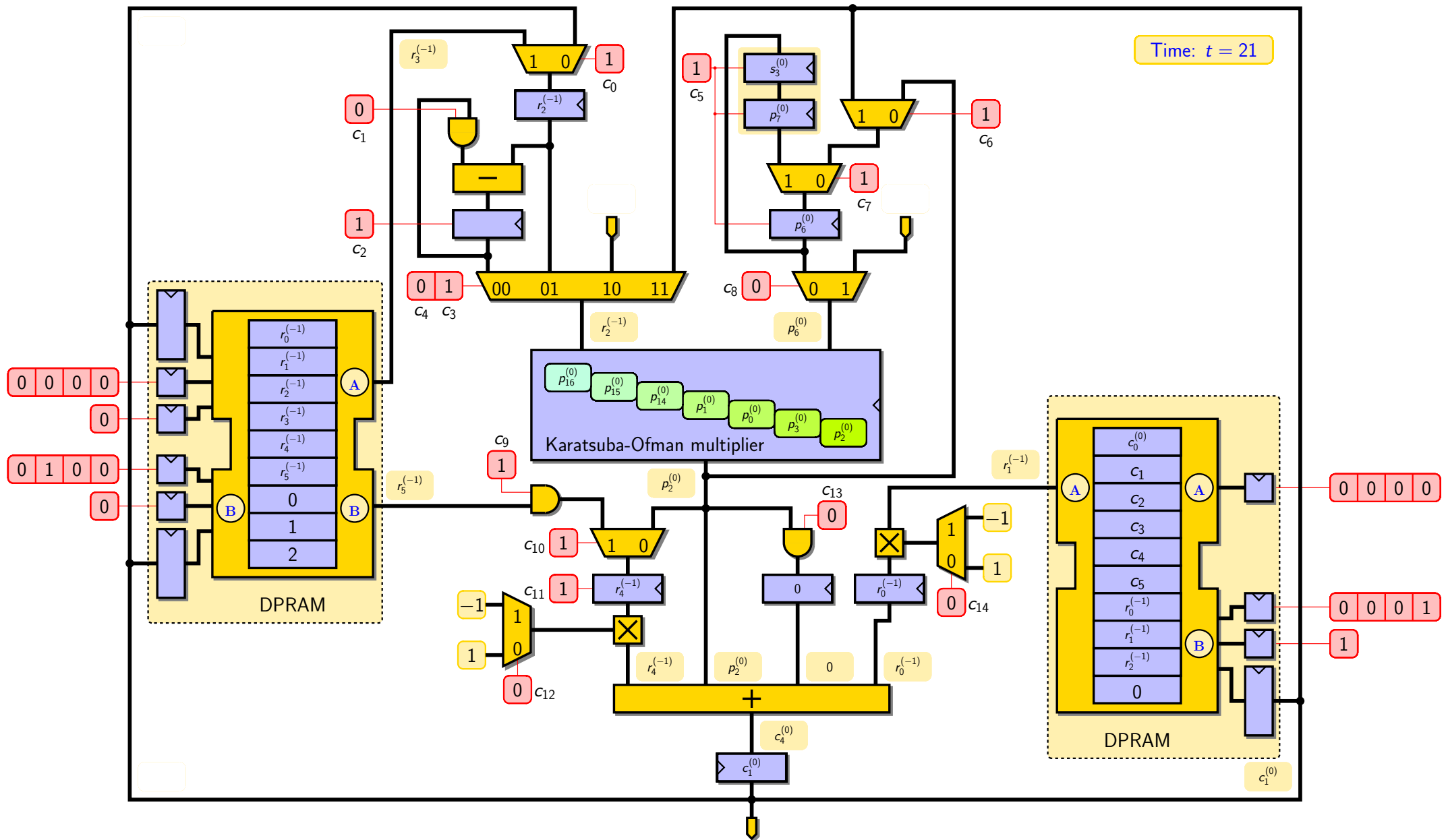
# Sparse Multiplication Over $\mathbb{F}_{36m}$



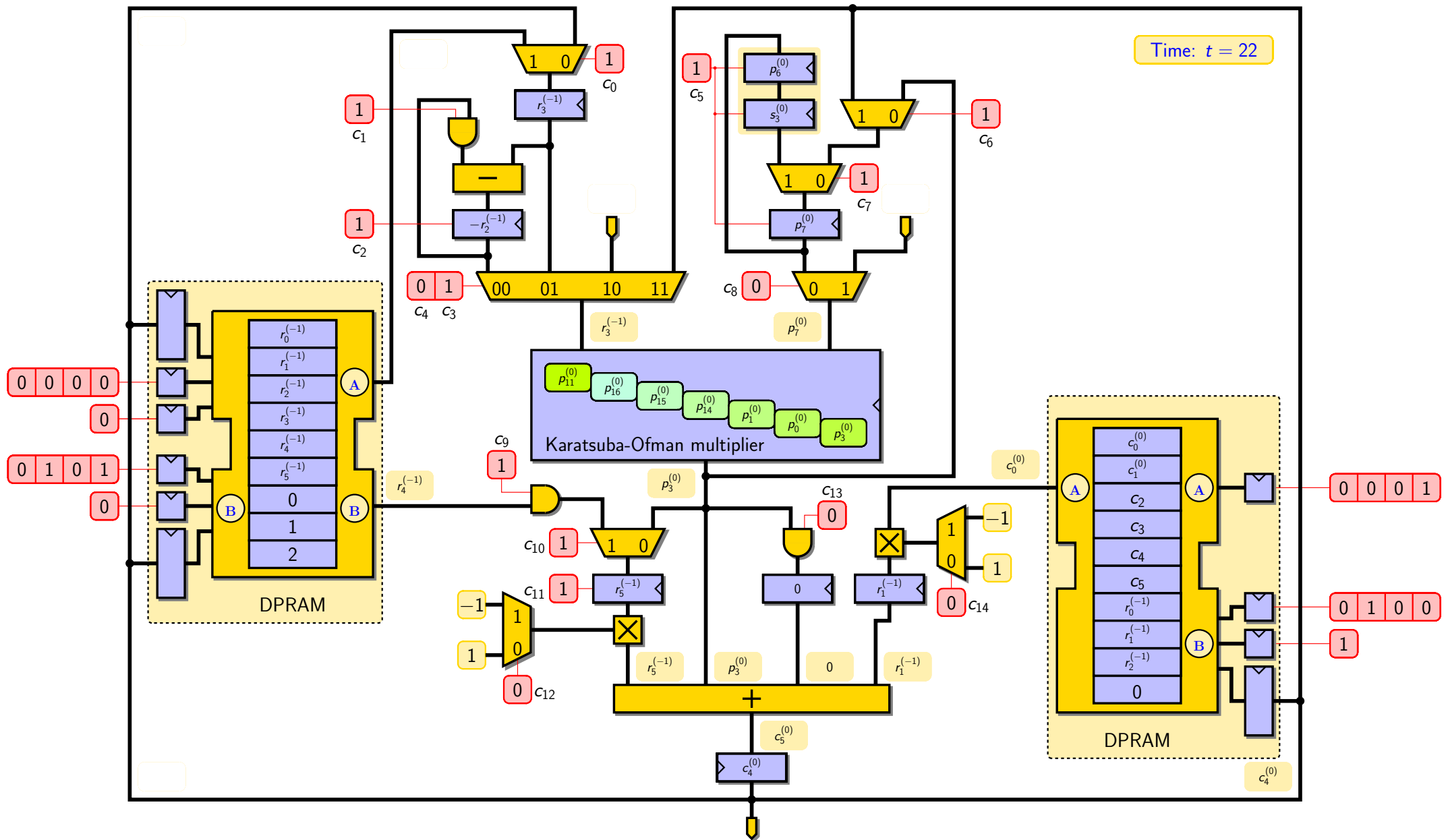
# Sparse Multiplication Over $\mathbb{F}_{36m}$



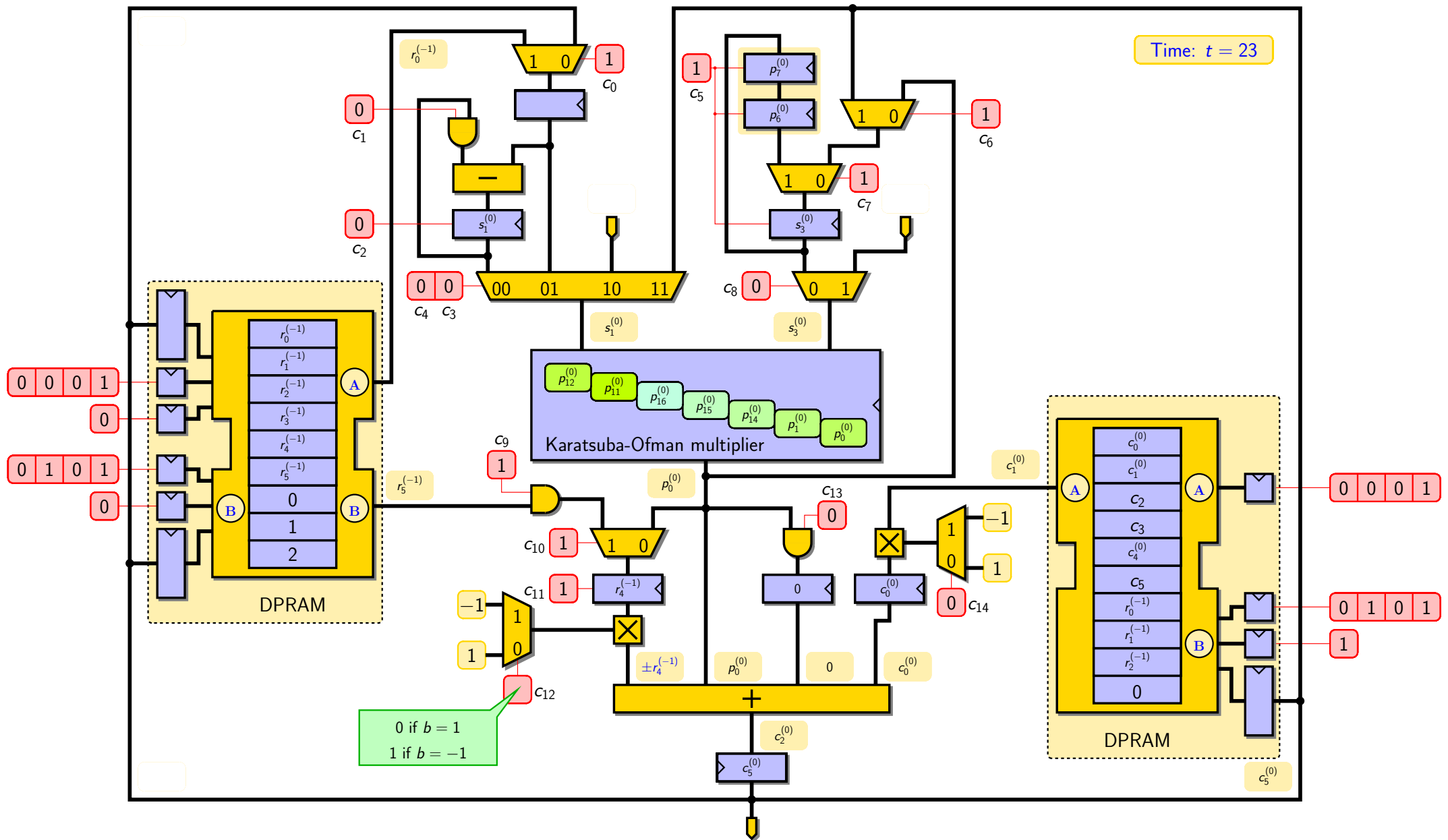
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



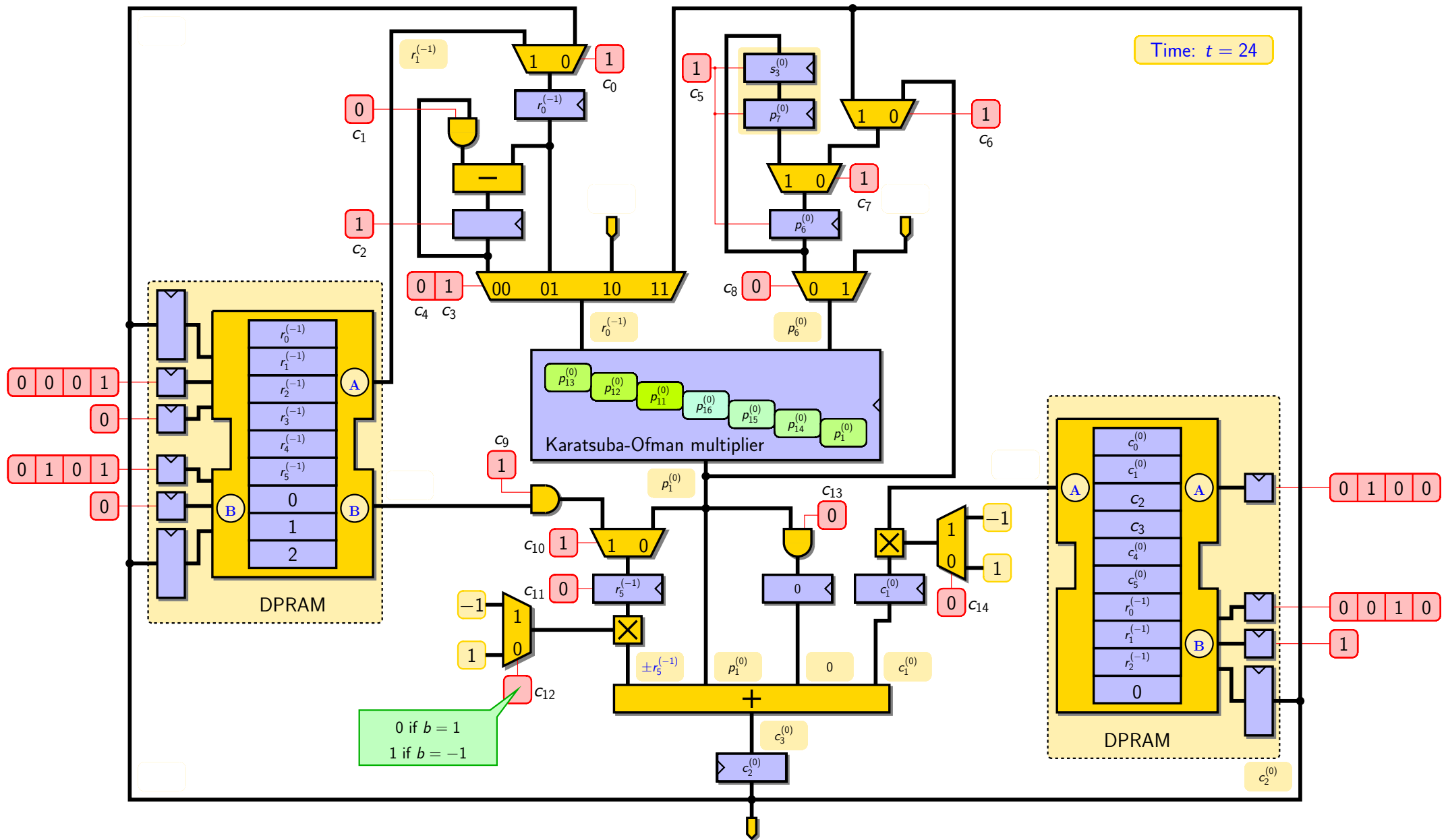
# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



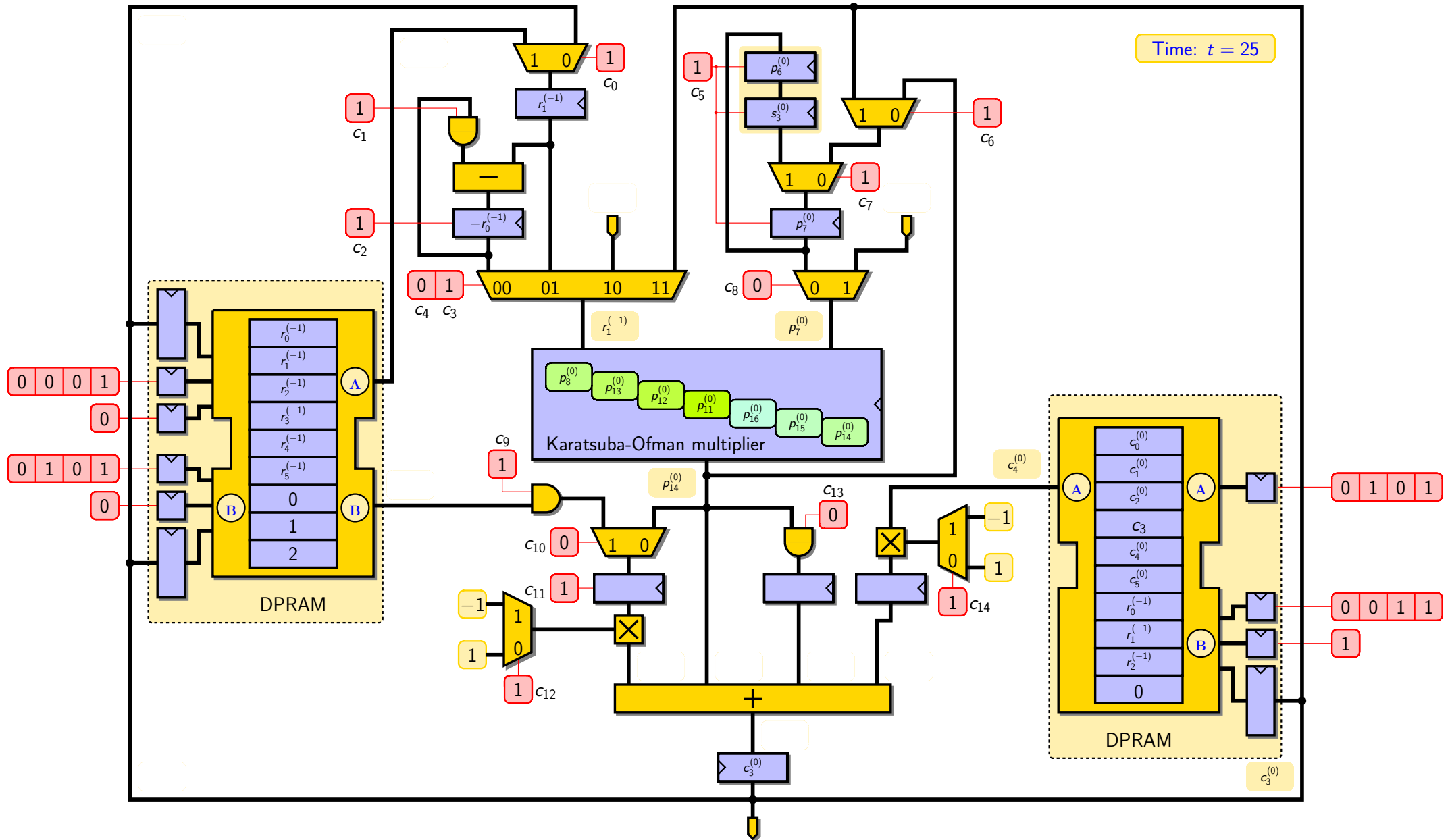
# Sparse Multiplication Over $\mathbb{F}_{36m}$



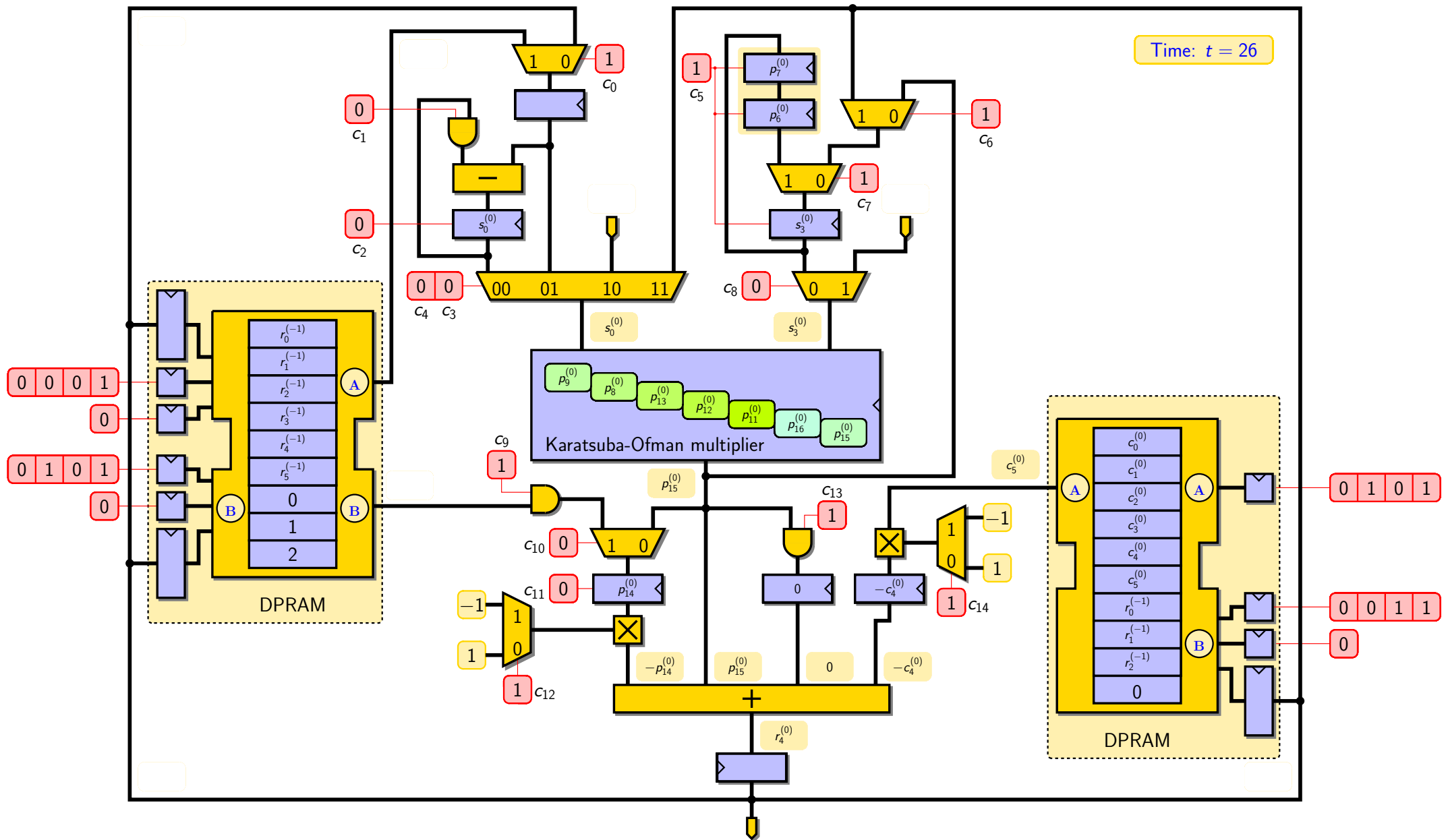
# Sparse Multiplication Over $\mathbb{F}_{36m}$



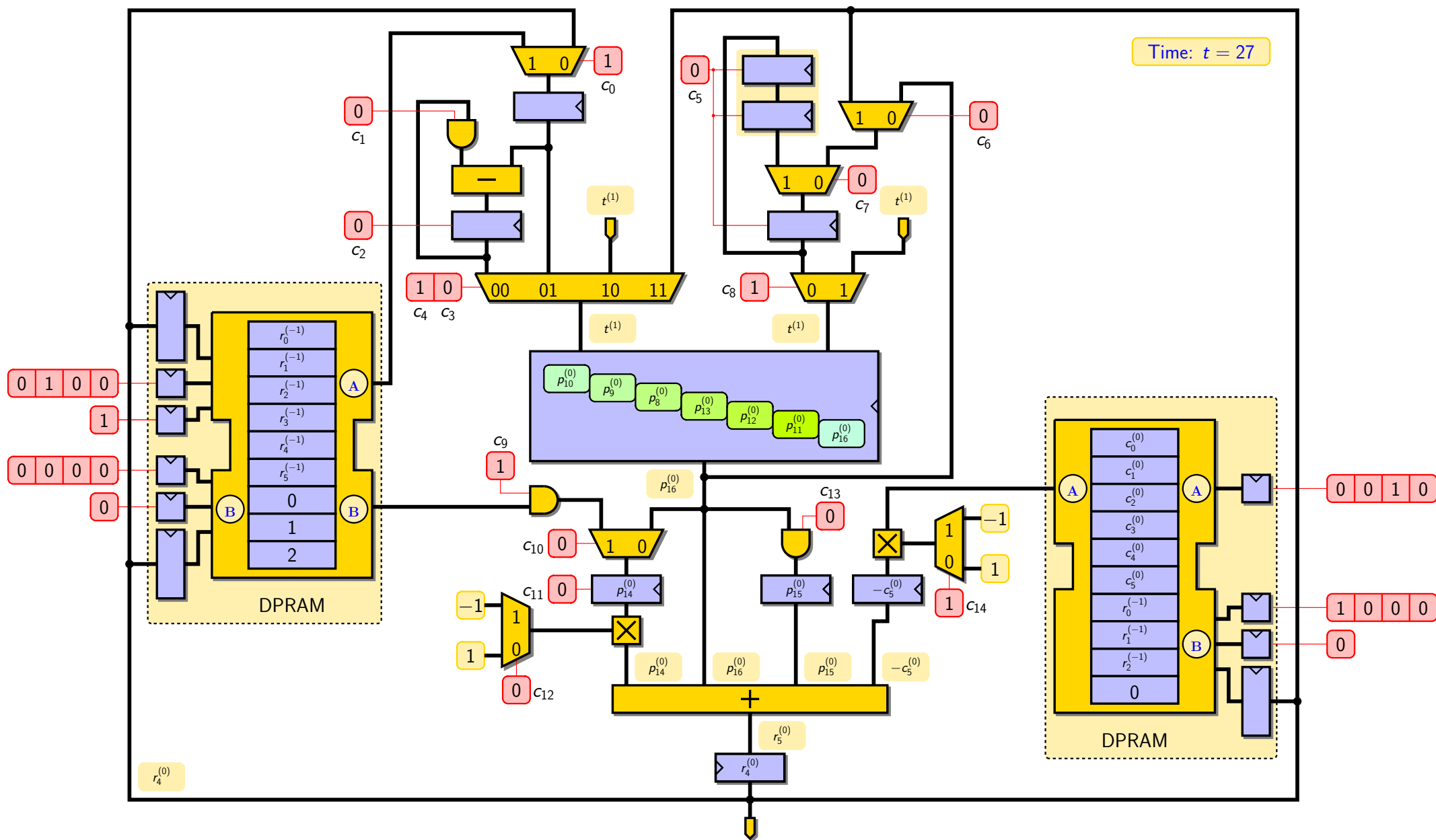
# Sparse Multiplication Over $\mathbb{F}_{36m}$



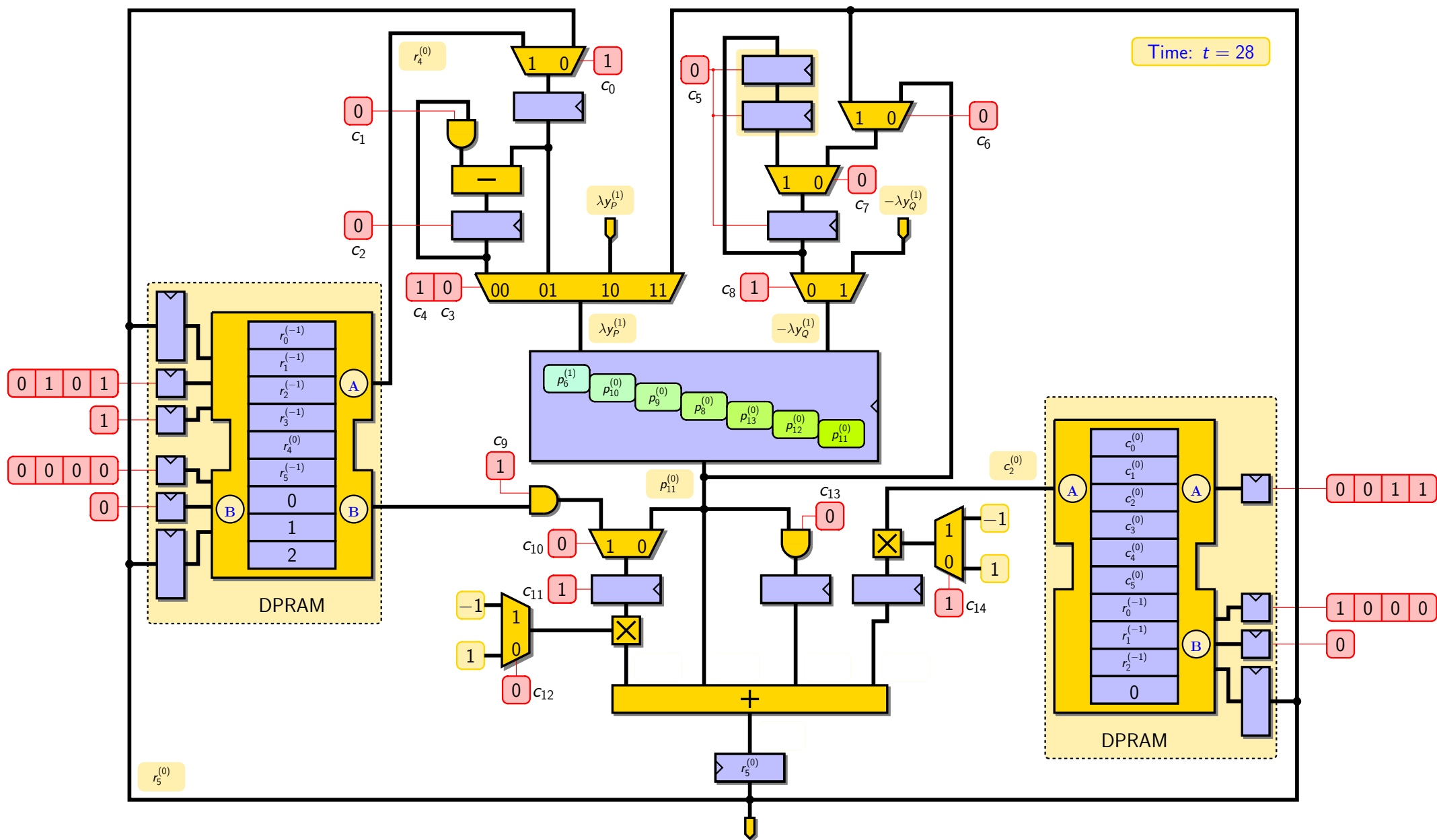
# Sparse Multiplication Over $\mathbb{F}_{36m}$



# Sparse Multiplication Over $\mathbb{F}_{36m}$

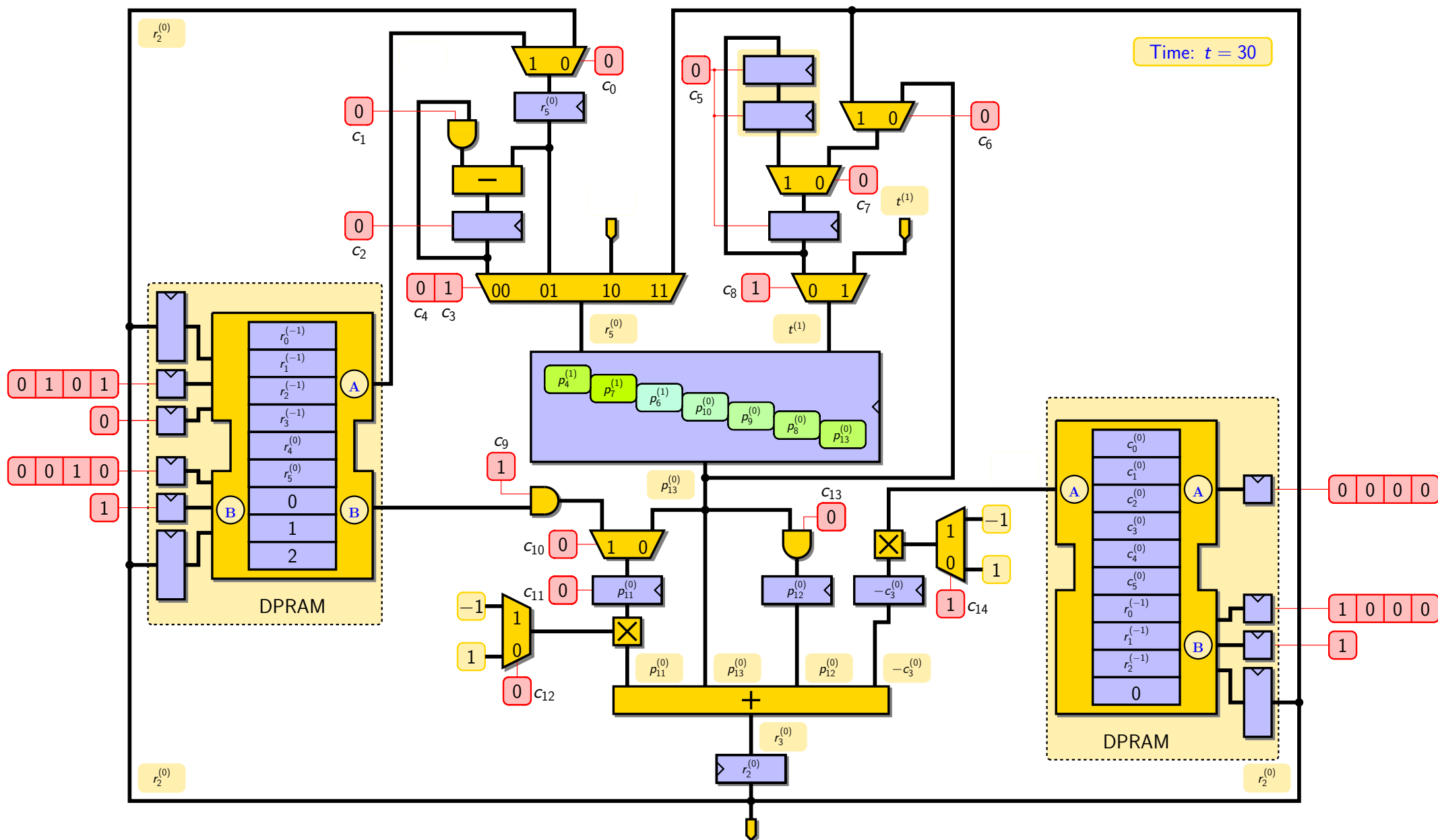


# Sparse Multiplication Over $\mathbb{F}_{36m}$

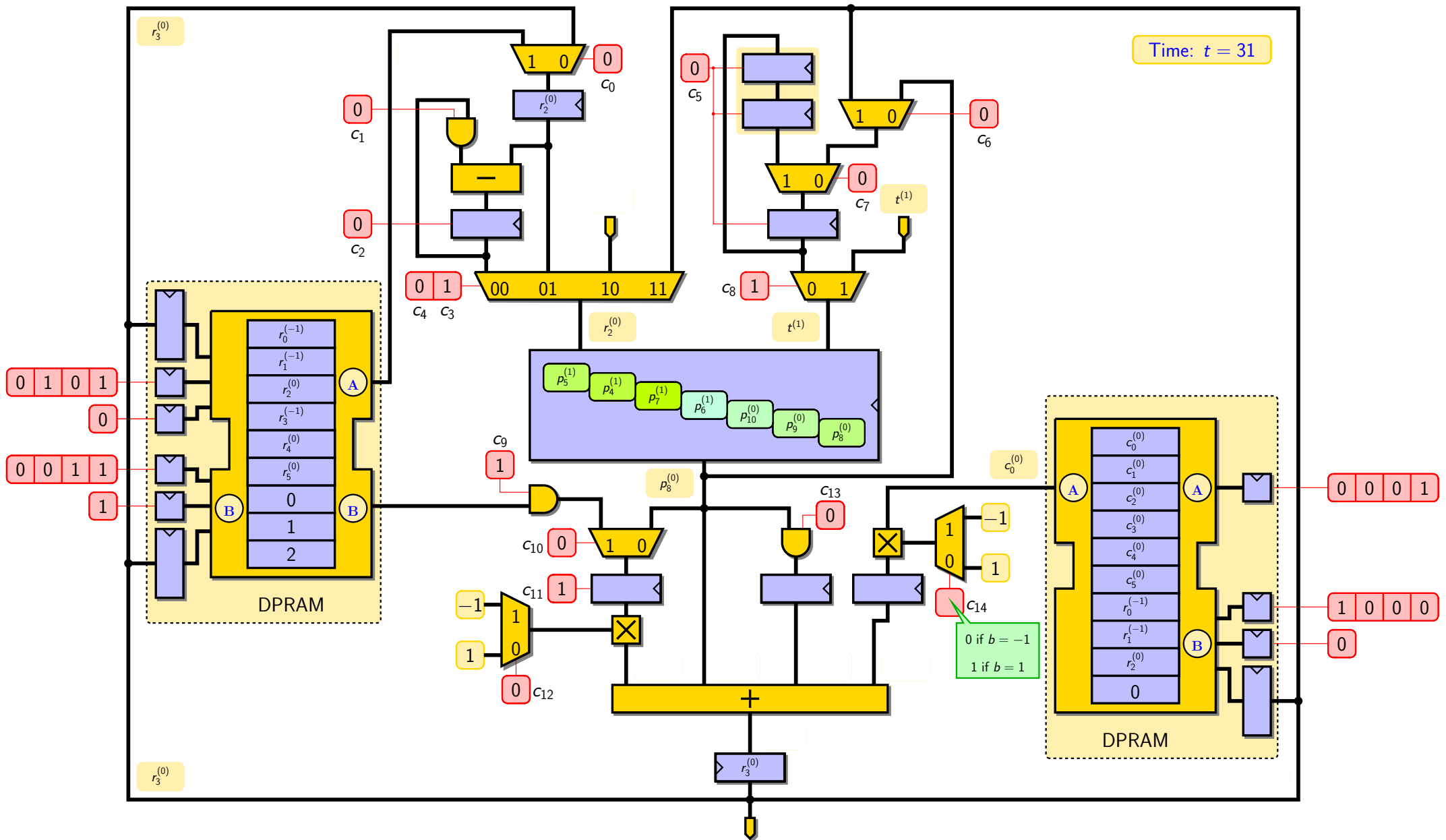




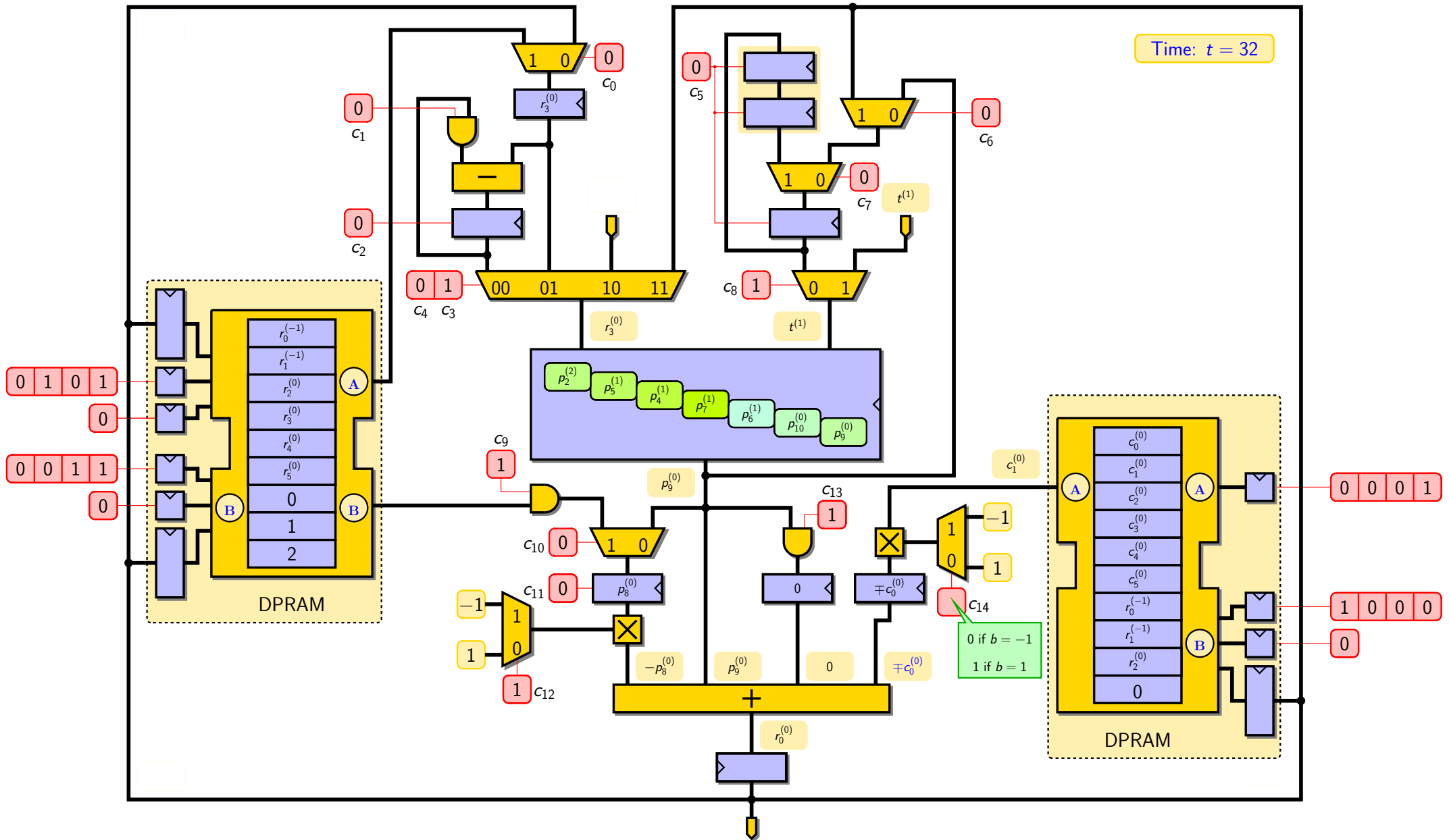
# Sparse Multiplication Over $\mathbb{F}_{36m}$



# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



# Sparse Multiplication Over $\mathbb{F}_{3^6m}$



# Sparse Multiplication Over $\mathbb{F}_{36m}$

