$\Sigma 0(x) = ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$

$\Sigma 1(x) = ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$

$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$

$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$

$K[t]$ – fixed consts from cubes of first 64 primes

9) Update Hash $H0 += a \bmod 2^{32}$, ..., etc and next 512 bit block

10) Concatate $H0 \| H1 \| \ldots \| H7$

# SHA-256

Blocks with 512 bits can be multiple

1) add 1 bit [1 - - - - - - -]
2) add 0 to len ≡ 448 mod 512
3) add 64 bit that is message length
4) „aaaa" - 4B = 4·8 bits = 32 bits
   32+1=33  k+33≡448 mod 512
   k≡448 -33 mod 512
   k≡415 mod 512
   → add 415 zeros

Final struct:
- data „aaaaaa" 32b
- „1" 1b
- 415 zeros 415b
- mesage len 64b

32+1+415+64=512

5) Split 512b in 16 32b blocks
   32b·16=512b
   16 words 4B
6) Expand to 64 words
   for t=16 to 63:

$$s_0 = (W_{t-15} >>> 7) \oplus (W_{t-15} >>> 18) \oplus (W_{t-15} >>> 3)$$
$$s_1 = (W_{t-2} >>> 17) \oplus (W_{t-2} >>> 19) \oplus (W_{t-2} >>> 10)$$
$$W_t = (W_{t-16} + s_0 + W_{t-7} + s_1) \bmod 2^{32}$$

7) H0=a; ...; H7=h
8) 64 rounds compresion

$$\{h=g; g=f; f=e; e=(d + T_1) \bmod 2^{32}; d=c; c=b; b=a; a=(T_1 + T_2) \bmod 2^{32}\}$$
$$T_1 = h + \Sigma_1^1(e) + Ch(e,f,g) + K[t] + W[t]$$
$$T_2 = \Sigma_1^0(a) + Maj(a,b,c)$$