total number of operations will be $O(bN)$ for N bits of data. Note that in the following implementation, the bit strings are stored in reverse order, with the first or highest-order bit occupying index 0, and the last or lowest-order bit at index nb:

Compute a Mod-2 Polynomial Checksum

```
mod2polychecksum( msg[], nb, mod2poly[], dm ):
[0] For n=0 to nb-dm-1, do [1] to [2]
[1]    If msg[n]==1, then do [2]
[2]       For d=0 to dm, replace msg[n+d] ^= mod2poly[dm-d]
[3] Let chksum = 0
[4] For n=nb-dm to nb-1, replace chksum = 2*chksum+msg[n]
[5] Return chksum
```

For CSG-1, suppose that $x(t)$ and $y(t)$ are mod-2 polynomials that differ at exactly one coefficient. Then $x(t) - y(t) = t^k$ for some nonnegative integer k, so $c_S(x) = c_S(y)$ if and only if $S(t)$ divides t^k. If $S(t)$ is irreducible and $\deg S > 1$, then this is impossible: $S(t)$ must divide t by Corollary 6.18, but then Lemma 6.15 gives the contradiction $\deg S \leq \deg t = 1$. For such S, c_S will detect all 1-bit errors.

For CSG-2, suppose that $x(t)$ and $y(t)$ differ at exactly two coefficients. Then $x(t) - y(t) = t^j(t^k + 1)$ for some integers $j \geq 0$ and $k > 0$. Thus $c_S(x) = c_S(y)$ if and only if $S(t)$ divides $t^j(t^k + 1)$ as a mod-2 polynomial. If $S(t)$ is irreducible and $\deg S > 1$, then $S(t)$ will not divide t^j for any j, as shown in the preceding paragraph. Thus, Corollary 6.18 implies that $c_S(x) = c_S(y)$ if and only if $S(t)$ divides $t^k + 1$, which it must do for some big enough k:

Theorem 6.19 *If $S(t)$ is any mod-2 polynomial not divisible by t, then there is an integer $N > 0$, depending on S, such that $S(t)$ divides $t^N + 1$, but $S(t)$ does not divide $t^k + 1$ for any integer $0 < k < N$.*

Proof: Consider the set $\{t^k \,\%\, S(t) : k = 0, 1, \ldots\}$, a subset of the mod-2 polynomials of degree less than $\deg S$. The set is finite, forcing $t^p = t^q \pmod{S(t)}$ for some integers $p > q \geq 0$. Since $S(t)$ is not divisible by t, $S(t)$ cannot divide t^k for any k. Thus $t^q \neq 0 \pmod{S(t)}$, so $t^{p-q} = 1 \pmod{S(t)}$. Since $1 + 1 = 0 \pmod{S(t)}$ we have found $n = p - q > 0$ such that $S(t)$ divides $t^n + 1$.

Since the set of positive integers $\{n : t^n = 1 \pmod{S(t)}\}$ is nonempty, it has a smallest element which we may call N. By construction, $S(t)$ does not divide $t^k + 1$ for any integer $0 < k < N$. □

Note that $S(t)$ is not divisible by t if and only if its integer value $S(2)$ is odd.

Let N be the minimal positive integer for an irreducible polynomial $S(t)$ not divisible by t. Then CSG-2 is achieved for all strings of N or fewer bits, as they correspond to mod-2 polynomials of degree $N - 1$ or less.

For checksum goals 3 and 4, detecting other bit errors, note that the mod-2 polynomial $S(t)$ yields 2^d different checksums,[10] where $d = \deg S$. Under the assumption that all values of $c_S(x)$ are equally likely with our potential bit strings

[10] Why doesn't it yield $S(2)$ checksums?