of linear functions. A function $h : \mathrm{F}^m \to \mathrm{F}$ is linear iff for every pair of points $(y_1, \ldots, y_m)$ and $(z_1, \ldots, z_m)$ in F^m it satisfies

$$h(y_1 + z_1, \ldots, y_m + z_m) = h(y_1, \ldots, y_m) + h(z_1, \ldots, z_m). \tag{4.14}$$

(The only if part of the statement is easy; the if part follows from Fact A.6 in the appendix.)

The procedure uses a stronger version of the above statement: if h satisfies the property in 4.14 for "most" pairs of m-tuples, then h is δ-close for some small δ.

Test for δ-closeness; Procedure 4.1-(i).

Given: $f : \mathrm{F}^m \to \mathrm{F}$ where $\mathrm{F} = \mathrm{GF}(2)$.

repeat $6/\delta$ times:
  Pick points y, z randomly from F^m.
  if $f(y) + f(z) \neq f(y + z)$
    /⋆ *Note: + on the left is addition mod* 2 *and*
    /⋆ *that on the right is componentwise addition mod* 2.
   exit and REJECT
exit and ACCEPT.

Complexity: The test requires $12m/\delta$ random bits, and reads $18/\delta$ values of f.

Correctness: Note that if $f \in \mathrm{F}_1[x_1, \ldots, x_m]$ then the test accepts with probability 1. According to the contrapositive to the next lemma, if f is not 3δ-close, then the basic step in the test fails with probability at least δ. Hence, after repeating the basic step $6/\delta$ times, the test rejects with probability close to $1 - 1/e^2$.

Theorem 4.13 ([BLR90]): *Let $F = GF(2)$ and f be a function from F^m to F such that when we pick y, z randomly from F^m,*

$$\Pr[f(y) + f(z) = f(y + z)] \geq 1 - \delta,$$

where $\delta < 1/6$. Then f is 3δ-close to some linear function.

Proof: The proof consists in three claims.

Claim 1: For every point $b \in \mathrm{F}^m$ there is a value $g(b) \in \{0, 1\}$ such that

$$\Pr_{w \in \mathrm{F}^m}[f(w + b) - f(w) = g(b)] \geq 1 - 2\delta.$$

Proof: Let $b \in \mathrm{F}^m$. Denote by p the probability $\Pr_w[f(w+b)-f(w)=1]$, where w is picked uniformly at random in F^m. Define random variables v_1, v_2 (taking values in F) as follows. Pick points $y, z \in \mathrm{F}^m$ randomly and independently from F^m, and let $v_1 = f(y+b) - f(y)$, and $v_2 = f(z+b) - f(z)$. Clearly, v_1, v_2 are independent random variables that take value 1 with probability p and 0 with probability $(1-p)$. The probability of the event "$v_1 = v_2$" is exactly $p^2 + (1-p)^2$. We show that actually this event happens with probability at least $1 - 2\delta$, whence it follows that either $p > 1 - 2\delta$ or $p < 2\delta$. If $p > 1 - 2\delta$, setting $g(b)$ to 1 fulfills the requirements of the lemma; in the other case, setting $g(b)$ to 0 does.

Note that + and − are the same over GF(2), so

$$\begin{aligned} v_1 - v_2 &= f(y+b) - f(y) - (f(z+b) - f(z)) \\ &= (f(z+y+b) - f(y+b)) + (f(z+y+b) - f(z+b)) - f(y) - f(z) \end{aligned}$$

Further, $y+b$ and $z+b$ are independently chosen random points. Hence the probability that each of the following two events happens is at least $1-\delta$: "$f(z+y+b) - f(y+b) = f(z)$", and "$f(z+y+b) - f(z+b) = f(y)$." So the probability that they both happen is at least $1 - 2\delta$, that is,

$$\Pr[(f(z+y+b) - f(y+b)) + (f(z+y+b) - f(z+b)) - f(y) - f(z) = 0] \geq 1 - 2\delta.$$

Thus $\Pr[v_1 = v_2] \geq 1 - 2\delta$, which finishes the proof of Claim 1.

Claim 2: The function g constructed in Claim 1 agrees with f in at least $1 - 3\delta$ fraction of b in F^m.

Proof: Let ρ be the fraction of points $b \in \mathrm{F}^m$ such that $f(b) = g(b)$.

Pick y, z randomly from F^m, and denote by A the event "$f(y+z) = g(y+z)$," and by B the event "$f(y) + f(y) = f(y+z)$." Note that A and B need not be independent. However, the hypothesis of the theorem implies that $\Pr[B] \geq 1 - \delta$. Further our assumption was that $\Pr[A] = \rho$. Now note that

$$\begin{aligned} \Pr[B] &= \Pr[B \wedge A] + \Pr[B \wedge \overline{A}] \\ &\leq \Pr[A] + \Pr[B \mid \overline{A}] \\ &\leq \rho + 2\delta \end{aligned}$$

where the last line uses the following implication of Claim 1:

$$\Pr[\text{“}f(y) + f(z) = f(y+z)\text{”} | \text{“}f(y+z) \neq g(y+z)\text{”}] \leq 2\delta.$$

But as we observed, $\Pr[B] \geq 1 - \delta$. Hence $\rho \geq 1 - 3\delta$. This finishes the proof of Claim 2.

Claim 3: Function g is linear, that is

$$\forall a, b \in \mathrm{F}^m, \quad g(a+b) = g(b) + g(a).$$

Proof: Fix arbitrary points $a, b \in \mathrm{F}^m$. To prove $g(a+b) = g(a)+g(b)$, it suffices to prove the existence of points $y, z \in \mathrm{F}^m$ such that each of the following is true: (i) $f(b+a+y+z)-f(y+z) = g(a+b)$ (ii) $f(b+a+y+z)-f(a+y+z) = g(b)$ and (iii) $f(a+y+z)-f(y+z) = f(a)$.

For, if (i), (ii) and (iii) are true for any $y, z \in \mathrm{F}^m$ then

$$\begin{aligned} g(b+a) &= f(b+a+y+z) - f(y+z) \\ &= f(b+a+y+z) - f(a+y+z) + f(a+y+z) - f(y+z) \\ &= g(b) + g(a) \end{aligned}$$

We prove the existence of the desired y, z in a probabilistic fashion. Choose y, z independently at random from F^m. The probability that any of (i), (ii), and (iii) is true is (by Claim 1) at least $1 - 2\delta$, and so the probability that all three are true is at least $1 - 6\delta$. Since $6\delta < 1$, the probability is strictly more than 0 that we obtain a pair y, z satisfying all the conditions of the claim. It follows that the desired pair y, z exists. This proves Claim 3.

Finally, note that Claims 2 and 3 imply (together with the fact in Equation 4.14) that f is $(1 - 3\delta)$-close.

□

Now we describe the other procedure connected with the linear function code.

Producing a value of $\tilde{f}$; Procedure 4.1-(ii).

Given: $f : \mathrm{F}^m \to \mathrm{F}$ that is δ-close; $\mathrm{F} = \mathrm{GF}(2)$.
Point $b \in \mathrm{F}^m$.

Pick random point y in F^m.
output $f(y+b) - f(y)$.

Complexity: The procedure uses $2m$ random bits and reads 2 values of f.

Correctness: If f is a linear function, then $f = \tilde{f}$, and $\Pr_y[f(y+b) - f(y) = \tilde{f}(b)] = 1$.

Now suppose f is just δ-close to some linear function. The following lemma shows that the procedure works correctly.

Lemma 4.14: $\Pr_y[f(y+b) - f(y) = \tilde{f}(b)] \geq 1 - 2\delta$.

Proof: Both y and $y+b$ are uniformly distributed in F^m (although they are not independent), hence

$$\Pr[f(y) = \tilde{f}(y)] \geq 1 - \delta \quad \text{and} \quad \Pr[f(y+b) = \tilde{f}(y+b)] \geq 1 - \delta.$$