

Supplement to
ON THE DISTRIBUTION OF k -DIMENSIONAL VECTORS
FOR SIMPLE AND COMBINED
TAUSWORTHE SEQUENCES

RAYMOND COUTURE, PIERRE L'ECUYER, AND SHU TEZUKA

6. EXAMPLES

In this section, a LS2 (or Tausworthe) generator g with multiplier a and modulus m will be denoted by $g = (a, m)$, and our use of Theorem 2 will always be with $h = k$ and $r = -l$.

6.1. A Combination of Two or Three Toy Generators. As a first illustration, we examine in detail the (low-dimensional) behavior of the three simple “toy” generators $g_1 = (x, x^3+x+1)$, $g_2 = (x^2, x^4+x+1)$, and $g_3 = (x^3, x^5+x^2+1)$, as well as the combination g_{23} of the last two, and the combination g_{123} of all three. Since $\gcd(2^5-1, 2^4-1) = \gcd(31, 15) = 1$, the period of g_{23} is $31 \times 15 = 465$. Similarly, since $\gcd(2^3-1, 465) = 1$, the period of g_{123} is $465 \times 7 = 3255$.

TABLE 7

Dimensions associated with g_1, g_2, g_3 , and their combinations, for $k = 2$.

l	d	d_{12}	d_{23}	d_{13}	d_1	d_2	d_3	D
1	10	5	7	6	1	2	3	2
2	8	3	5	4	0	0	1	3
3	6	2	3	2	0	0	0	2
4	4	1	2	1	0	0	0	1
5	2	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0

TABLE 8

Values of $\varphi_l(n)$ for g_1, g_2 , and g_3 , for $k = 2$.

g_1			g_2			g_3		
l	n	$\varphi_l(n)$	l	n	$\varphi_l(n)$	l	n	$\varphi_l(n)$
1	2	3	1	4	3	1	8	3
	1	1		3	1		7	1
	0	0		0	0		0	0
2	1	7	2	1	15	2	2	15
	0	9		0	1		1	1
							0	0
						3	1	31
							0	33

empty cells and also cells that contain more than one point. Note that for $l = 1$ and 2 , the number of cells with 2^d points turns out to be zero. That kind of situation happens quite frequently. For g_{23} , $d = p - lk$ holds for l up to 6 . After that, any cell will contain either 0 or 1 point. Observe that the values of d , d_1 , or d_2 , never increase when l increases. But this does not necessarily hold for D .

TABLE 9
Values of $\varphi_l(n)$ for g_{23} and g_{123} , for $k = 2$.

g_{23}			g_{123}		
l	n	$\varphi_l(n)$	l	n	$\varphi_l(n)$
1	117	1	1	814	3
	116	3		813	1
	0	0		0	0
2	30	1	2	204	7
	29	15		203	9
	0	0		0	0
3	8	24	3	53	16
	7	33		52	16
	6	7		51	3
	0	0		50	5
4	4	84		49	20
	3	41		48	4
	2	3		0	0
	0	128	4	16	48
5	2	210		14	64
	1	45		13	4
	0	769		12	60
				11	33
				10	35
				9	10
				8	2
				0	0
			5	4	504
				3	246
				2	228
				1	45
				0	1
			6	1	3255
				0	841

TABLE 10
Dimensions d , d_2 , d_3 , and values of $\varphi_l(n)$ for g_{23} , for $k = 3$.

l	d	d_2	d_3
1	59	1	
	58	7	
	0	0	
2	8	24	
	7	33	
	6	7	
	0	0	
3	1	465	
	0	47	

Table 10 gives the values that correspond to g_{23} in dimension $k = 3$. One has $d = p - lk$ for $l \leq 3$. Despite that, for $l = 3$, there are 47 empty cells, owing to the fact that in this case, $n = 0$ for lines 2, 3, and 5 in Table 4.

Figure 1 shows all the points produced by the generator g_{23} , in dimension $k = 2$. This illustrates the results of the left-hand part of Table 9. For example, the grid on the figure partitions the square into $2^6 = 64$ cells, which corresponds to $l = 3$. As indicated by Table 9, 24 cells contain 8 points, 33 cells contain 7 points, and 7 cells contain 6 points. If the grid were refined to partition the square into $2^8 = 256$ cells (i.e., $l = 4$), then, as indicated by Table 9, there would be 128 empty cells while the other cells would contain either 2, 3, or 4 points.

Table 7 gives all the kernel dimensions referred to in Tables 1–6, for $k = 2$. These have been computed using Theorem 2 and Lemma 3. From these values, we have computed the $\varphi_l(n)$'s for different values of l , for the generators g_1 , g_2 , g_3 , and g_{123} . These are given in Tables 8 and 9. One can see that g_1 , g_2 , and g_3 reach the best possible resolution considering their period length, for all l . But their periods are very small. For the combination g_{23} , one has $d = p - lk$ (and maximum resolution) only for $l \leq 3$. For $l = 4$ and $l = 5$, there are

TABLE 11
The values of d in dimensions $k = 2$ to 10 , for generator g_A .

l	k									
	2	3	4	5	6	7	8	9	10	
1	30	29	28	27	26	25	24	23	22	
2	28	26	24	22	20	18	16	14	12	
3	26	23	20	17	14	11	8	5	2	
4	24	20	16	12	8	4	1	-	-	
5	22	17	12	7	2	-	-	-	-	
6	20	14	8	2	-	-	-	-	-	
7	18	11	4	-	-	-	-	-	-	
8	16	8	-	-	-	-	-	-	-	
9	14	5	-	-	-	-	-	-	-	
10	12	2	-	-	-	-	-	-	-	
11	10	1	-	-	-	-	-	-	-	
12	8	-	-	-	-	-	-	-	-	
13	6	-	-	-	-	-	-	-	-	
14	4	-	-	-	-	-	-	-	-	
15	2	-	-	-	-	-	-	-	-	
16	1	-	-	-	-	-	-	-	-	

TABLE 12
Values of $\varphi_i(n)$ for g_A in dimensions $k = 2, 3$, and 8 .

k = 2			k = 3			k = 8		
l	n	$\varphi_l(n)$	l	n	$\varphi_l(n)$	l	n	$\varphi_l(n)$
14	16	$2^{28} - 1$	9	32	$2^{27} - 1$	2	2^{16}	$2^{16} - 1$
	15	1		31	1		$2^{16} - 1$	1
15	4	$2^{30} - 1$	10	4	$2^{30} - 1$	3	2^8	$2^{24} - 1$
	3	1		3	1		$2^8 - 1$	1
16	2	$2^{31} - 1$	11	2	$2^{31} - 1$	4	2	$2^{31} - 1$
	1	1		1	1		1	1
	0	2^{31}		0	2^{31}		0	2^{31}

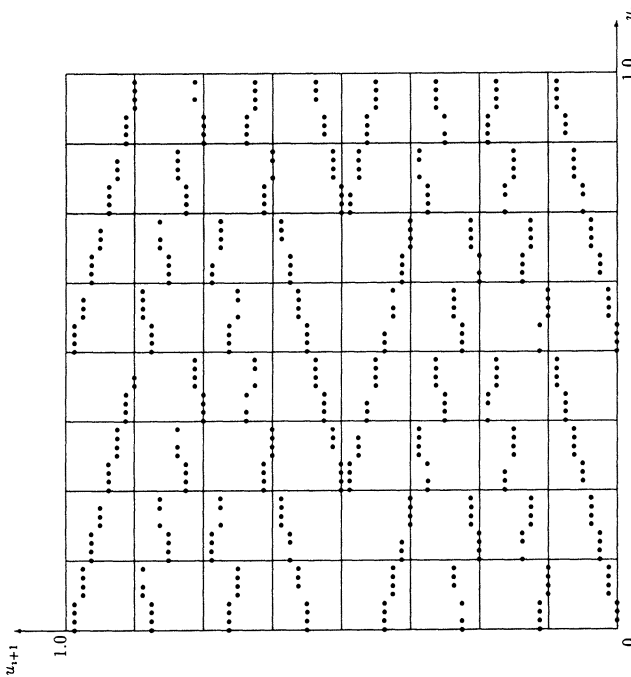


FIGURE 1
The pairs (u_i, u_{i+1}) , produced by the combined Tausworthe generator g_{23} .

6.2. A Simple Generator From André, Mullen, and Niederreiter. We now examine a simple Tausworthe generator based on a polynomial of degree $p = 32$, which has been obtained by André et al. [1] and was called "universally optimal". This generator is $g_A = (x^{32}, x^{32} + x^{30} + x^{28} + x^{27} + x^{26} + x^{24} + x^{22} + x^{21} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. Table 11 gives the values of d for all dimensions $k \leq 10$, and all l . For $l > 16$ and for the entries marked "n", one has $d = 0$. There are only three nonzero entries for which $d > p - lk$, i.e., for which one does not have k -distribution with resolution l , and these are the three entries with $d = 1$. Table 12 shows what happens with the values of Table 1 for each of these three cases: there are 2^{31} empty cells and $2^{31} - 1$ cells that contain two points each.

6.3. A Simple Generator From Mullen and Niederreiter. Here, we look at another so-called "optimal polynomial", suggested in Mullen and Niederreiter [9]. This one has degree 64 and yields the generator $g_M = (x^{64}, x^{64} + x^{58} + x^{54} + x^{49} + x^{32} + 1)$. This polynomial was designed to be optimal only relative to the 2-dimensional distribution. So, it is not necessarily expected to behave well in higher dimensions. Table 13 gives the values of d for all dimensions $k \leq 5$, and all $l \geq 11$. For $k = 3$, one has $d > p - lk$ for all $l \geq 17$. Also, $d > p - lk$ for $k = 5$ and $l = 13$. Table 14 shows what happens with $\varphi_i(n)$ in dimension $k = 3$. For example, with $l = 21$, one has approximately 2^{63} empty cells and 2^{53} cells that contain 2^{11} points each. This is not very good.

TABLE 13
The values of d in dimensions
 $k = 2$ to 5 , for generator g_M .

l	k				
	2	3	4	5	-
11	42	31	20	9	-
12	40	28	16	4	-
13	38	25	12	1	-
14	36	22	8	-	-
15	34	19	4	-	-
16	32	16	-	-	-
17	30	15	-	-	-
18	28	14	-	-	-
19	26	13	-	-	-
20	24	12	-	-	-
21	22	11	-	-	-
22	20	10	-	-	-
23	18	9	-	-	-
24	16	8	-	-	-
25	14	7	-	-	-
26	12	6	-	-	-
27	10	5	-	-	-
28	8	4	-	-	-
29	6	3	-	-	-
30	4	2	-	-	-
31	2	1	-	-	-
32	-	-	-	-	-

TABLE 14
Values of $\varphi_i(n)$ for g_M
in dimension $k = 3$.

l	$k = 3$	
	n	$\varphi_i(n)$
16	2^{16}	$2^{48} - 1$
	$2^{16} - 1$	1
17	2^{15}	$2^{49} - 1$
	$2^{15} - 1$	1
	0	$2^{51} - 2^{49}$
18	2^{14}	$2^{50} - 1$
	$2^{14} - 1$	1
	0	$2^{54} - 2^{50}$
19	2^{13}	$2^{51} - 1$
	$2^{13} - 1$	1
	0	$2^{57} - 2^{51}$
20	2^{12}	$2^{52} - 1$
	$2^{12} - 1$	1
	0	$2^{60} - 2^{52}$
21	2^{11}	$2^{53} - 1$
	$2^{11} - 1$	1
	0	$2^{63} - 2^{53}$

6.4. A Combined Tausworthe Generator Taken From SUPER-DUPER. Our last example is a combined Tausworthe generator, which is itself a component of the generator Super-Duper proposed by Marsaglia et al. [8]. This generator is given by $g = (x^{32}, x^{32} + x^{15} + 1)$. Note that $M(x) = x^{32} + x^{15} + 1$ is not irreducible and can be written as $M(x) = (x^{21} + x^{19} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1)(x^{11} + x^9 + x^7 + x^2 + 1)$. So, this generator can be regarded as a combined Tausworthe generator. The maximum possible period is $(2^{21} - 1)(2^{11} - 1)$ and thereby almost all initial values give the maximum period. Table 15 gives the values of d , d_1 , and d_2 for all l , in dimensions 2 to 4. From that, one can use Table 4 to compute $\varphi_l(n)$. The results are given in Table 16. Here, the values for which maximum resolution ($d = p - lk$) is not attained are $l = 16$ for $k = 2$, and all $l \geq 3$ for $k = 3$ and 4. Therefore, bad behavior is to be expected in dimensions 3 and 4. Table 16 confirms that. For example, in dimension 3 and with $l = 6$, there are 245760 empty cells, 2047 cells that contain 262015 points each, and 14337 cells that contain 262016 points each.

TABLE 15
Values of d , d_1 , and d_2 for the component of Super-Duper.

l	$k = 2$			$k = 3$			$k = 4$				
	d	d_1	d_2	d	d_1	d_2	d	d_1	d_2		
1	30	19	9	1	29	18	8	1	28	17	7
2	28	17	7	2	26	15	5	2	24	13	3
3	26	15	5	3	24	13	3	3	22	11	1
4	24	13	3	4	22	11	1	4	20	9	0
5	22	11	1	5	20	9	0	5	18	7	0
6	20	9	0	6	18	7	0	6	16	5	0
7	18	7	0	7	16	5	0	7	14	3	0
8	16	5	0	8	14	3	0	8	12	1	0
9	14	3	0	9	12	1	0	9	10	0	0
10	12	1	0	10	10	0	0	10	8	0	0
11	10	0	0	11	10	0	0	11	8	0	0
12	8	0	0	12	8	0	0	12	6	0	0
13	6	0	0	13	6	0	0	13	6	0	0
14	4	0	0	14	4	0	0	14	4	0	0
15	2	0	0	15	2	0	0	15	2	0	0
16	1	0	0	16	1	0	0	16	1	0	0

APPENDIX

TABLE 16
Values of $\varphi_i(n)$ for the component of Super-Duper.

$k = 2$		$\varphi_i(n)$
l	n	
14	16	$2^{28} - 2^{21} - 2^{11} + 16$
	15	$2^{21} + 2^{11} - 2^5 + 1$
	14	15
15	4	$2^{30} - 2^{21} - 2^{11} + 4$
	3	$2^{21} + 2^{11} - 7$
2		3
16	2	$2^{31} - 2^{21} - 2^{11} + 2$
	1	$2^{21} + 2^{11} - 3$
	0	$2^{31} + 1$

$k = 3$		$\varphi_i(n)$
l	n	
2	$2^{26} - 2^{18} - 2^5$	$2^6 - 1$
	$2^{26} - 2^{15} - 2^5 + 1$	1
3	$2^{24} - 2^{15} - 2^3$	$2^8 - 1$
	$2^{24} - 2^{13} - 2^3 + 1$	1
	0	2^8
4	$2^{22} - 2^{11} - 2$	$2^{10} - 1$
	$2^{22} - 2^{11} - 1$	1
	0	$2^{12} - 2^{10}$
5	$2^{20} - 2^9$	$2^{12} - 2^{11} + 1$
	$2^{20} - 2^9 - 1$	$2^{11} - 1$
	0	$2^{15} - 2^{12}$
6	$2^{18} - 2^7$	$2^{14} - 2^{11} + 1$
	$2^{18} - 2^7 - 1$	$2^{11} - 1$
	0	$2^{18} - 2^{14}$

$k = 4$		$\varphi_i(n)$
l	n	
2	$2^{24} - 2^{13} - 2^3$	$2^8 - 1$
	$2^{24} - 2^{13} - 2^3 + 1$	1
3	$2^{22} - 2^{11} - 2$	$2^{10} - 1$
	$2^{22} - 2^{11} - 1$	1
	0	$2^{12} - 2^{10}$
4	$2^{20} - 2^9$	$2^{12} - 2^{11} + 1$
	$2^{20} - 2^9 - 1$	$2^{11} - 1$
	0	$2^{16} - 2^{12}$
5	$2^{18} - 2^7$	$2^{14} - 2^{11} + 1$
	$2^{18} - 2^7 - 1$	$2^{11} - 1$
	0	$2^{20} - 2^{14}$
6	$2^{16} - 2^5$	$2^{16} - 2^{11} + 1$
	$2^{16} - 2^5 - 1$	$2^{11} - 1$
	0	$2^{24} - 2^{16}$

In this appendix, we derive a technical result that was used in the proof of Lemma 3 in §5.3. Let $V = V_1 + V_2 + V_3$ be a direct sum of vector spaces and $W \subset V$ a subspace. For each $i \neq j$, let $W_i = W \cap V_i$, $W_{ij} = W \cap (V_i + V_j)$, $d = \dim(W)$, $d_i = \dim(W_i)$, and $d_{ij} = \dim(W_{ij})$. Let

$$\tilde{W} = W_{12} + W_{13} + W_{23}$$

and $\tilde{d} = \dim(\tilde{W})$. Let $D = \dim(((V_1 + W) \cap (V_2 + W) \cap (V_3 + W)) / W)$. Our aim is now to express D as a function of quantities defined above.

Let $W_0 = W_1 + W_2 + W_3$, and for each subspace E of V , let \tilde{E} denote the image of E by the canonical mapping $V \rightarrow V/W_0$. We will perform a reduction of everything modulo W_0 . The development will then be easier in space \tilde{V} , owing to the fact that $\tilde{W} \cap \tilde{V}_i = \tilde{W}_i = \{0\}$ for each i . For each i and $j \neq i$, one has the following:

$$\begin{aligned} \tilde{V} &= \tilde{V}_1 + \tilde{V}_2 + \tilde{V}_3 \text{ (direct sum),} \\ \tilde{W}_i &= \tilde{W} \cap \tilde{V}_i = \{0\}; \\ \tilde{W}_{ij} &= \tilde{W} \cap (\tilde{V}_i + \tilde{V}_j), \\ d_{ij} &\stackrel{\text{def}}{=} \dim(\tilde{W}_{ij}) = \dim(\tilde{W} \cap (\tilde{V}_i + \tilde{V}_j)) = \dim(W_{ij}) - \dim(W_{ij} \cap W_0) \\ &= \dim(W_{ij}) - \dim(W_i + W_j) = d_{ij} - d_i - d_j, \\ \tilde{d} &\stackrel{\text{def}}{=} \dim(\tilde{W}) = \dim(W) - \dim(W_0) = d - d_1 - d_2 - d_3. \end{aligned} \tag{23}$$

One has $\tilde{W} \stackrel{\text{def}}{=}} \sum_{i \neq j} \tilde{W}_{ij} = \tilde{W}$ and

$$\tilde{d} \stackrel{\text{def}}{=} \dim(\tilde{W}) = \tilde{d} - d_1 - d_2 - d_3. \tag{24}$$

Finally,

$$(25) \quad \dim((V_1 + W) \cap (V_2 + W) \cap (V_3 + W)) = \dim((\tilde{V}_1 + \tilde{W}) \cap (\tilde{V}_2 + \tilde{W}) \cap (\tilde{V}_3 + \tilde{W})) + d_1 + d_2 + d_3.$$

Let $H_1 = \tilde{V}_1 \cap (\tilde{V}_2 + \tilde{W}_{12}) \cap (\tilde{V}_3 + \tilde{W}_{13})$.

Lemma 4. One has

$$(26) \quad (\tilde{V}_1 + \tilde{W}) \cap (\tilde{V}_2 + \tilde{W}) \cap (\tilde{V}_3 + \tilde{W}) = H_1 + \tilde{W}$$

and $D = \dim(H_1)$.

Proof. Let $v_1 + w_1 = v_2 + w_2 = v_3 + w_3$ be a common element to the three spaces that intersect on the left in equation (26). One then has $v_1 = v_2 + (w_2 - w_1) = v_3 + (w_3 - w_1)$, where $w_2 - w_1 \in \tilde{W}_{12}$ and $w_3 - w_1 \in \tilde{W}_{13}$. Therefore, v_1 belongs to H_1 and the set on the left is a subset of the one on the right. The inclusion in the other direction is immediate.

Since $H_1 \subset \check{V}_1$, we have that $H_1 \cap \check{W}$ is a subset of \check{W}_1 and is therefore $\{0\}$. This means that the sum $H_1 + \check{W}$ is direct. Then, from (26) and (25), one has

$$\begin{aligned} D &= \dim((\check{V}_1 + \check{W}) \cap (\check{V}_2 + \check{W}) \cap (\check{V}_3 + \check{W})) + d_1 + d_2 + d_3 - d \\ &= \dim(H_1) + \dim(\check{W}) + d_1 + d_2 + d_3 - d \\ &= \dim(H_1). \quad \square \end{aligned}$$

Let π_i denote the canonical projection $\check{V} \mapsto \check{V}_i$. Since $\check{W}_i = \{0\}$, for each $v_1 \in H_1$ there are unique elements $w_{12} \in \check{W}_{12}$ and $w_{13} \in \check{W}_{13}$ such that $\pi_1(w_{12}) = \pi_1(w_{13}) = v_1$. We can then define a linear mapping $\mu : H_1 \mapsto \check{W}_{23}$ by $\mu(v_1) = \pi_2(w_{12}) - \pi_3(w_{13}) (= w_{12} - w_{13})$, since $\pi_1(w_{12} - w_{13}) = 0$.

Lemma 5. *The mapping μ is one-to-one and $\mu(H_1) = (\check{W}_{12} + \check{W}_{13}) \cap \check{W}_{23}$.*

Proof. If $\mu(v_1) = 0$, then $w_{12} = w_{13} \in (\check{V}_1 + \check{V}_2) \cap (\check{V}_1 + \check{V}_3) = \check{V}_1$, so that $w_{12} = w_{13} = 0$ and $v_1 = \pi_1(w_{12}) = 0$. This implies that μ is one-to-one. By construction, we have $\mu(H_1) \subset (\check{W}_{12} + \check{W}_{13}) \cap \check{W}_{23}$, and it remains to show the reverse inclusion. Let $w_{23} = w_{12} - w_{13} \in (\check{W}_{12} + \check{W}_{13}) \cap \check{W}_{23}$ and $v = \pi_1(w_{23}) = 0$, we have $\pi_1(w_{13}) = \pi_1(w_{12}) = v$ and $v \in H_1$. Then, from the definition of μ , $\mu(v) = w_{23}$, and this completes the proof. \square

Lemma 6. *We have*

$$\begin{aligned} D &= \dim(H_1) = \check{d}_{12} + \check{d}_{13} + \check{d}_{23} - \dim(\check{W}) \\ (27) \quad &= d_{12} + d_{13} + d_{23} - d_1 - d_2 - d_3 - \check{d}. \end{aligned}$$

Proof. Keeping in mind that the sum $\check{W}_{12} + \check{W}_{13}$ is direct because each \check{W}_i is $\{0\}$, and using the previous lemma, one has

$$\begin{aligned} \dim(\check{W}) &= \dim(\check{W}_{12} + \check{W}_{13} + \check{W}_{23}) \\ &= \dim(\check{W}_{23}) + \dim(\check{W}_{12} + \check{W}_{13}) - \dim((\check{W}_{12} + \check{W}_{13}) \cap \check{W}_{23}) \\ &= \check{d}_{23} + \check{d}_{12} + \check{d}_{13} - \dim(H_1). \end{aligned}$$

This gives the middle equality. The first equality is already contained in Lemma 4, while the last one follows from (23) and (24). \square

The following example shows that knowing d , the d_i 's, and d_{ij} 's is not sufficient in general to compute D .

Example. For $i = 1, 2, 3$, let $\dim(V_i) = 2$ and let $\{v_i, v_i'\}$ be a basis for V_i . We consider two cases. In the first case, suppose that $W = \mathbb{F}_2 \cdot (v_1 + v_2') + \mathbb{F}_2 \cdot (v_2 + v_3') + \mathbb{F}_2 \cdot (v_3 + v_1')$, where $\mathbb{F}_2 \cdot v$ means the space $\{0, v\}$. Then, $W_i = W \cap V_i = \{0\}$ for each i and $H_i = V_i \cap (V_2 + W_{12}) \cap (V_3 + W_{13}) = V_i \cap (V_2 + \mathbb{F}_2 \cdot (v_1 + v_2')) \cap (V_3 + \mathbb{F}_2 \cdot (v_3 + v_1')) = V_i \cap (V_2 + \mathbb{F}_2 \cdot v_1) \cap (V_3 + \mathbb{F}_2 \cdot v_1) = \{0\}$, so that $D = \dim(H_1) = 0$. In the second case, suppose that $W = \mathbb{F}_2 \cdot (v_1 + v_2) + \mathbb{F}_2 \cdot (v_2 + v_3) + \mathbb{F}_2 \cdot (v_1' + v_2' + v_3')$. Then, $W \cap V_i = \{0\}$ for each i and $H_1 = V_1 \cap (V_2 + W_{12}) \cap (V_3 + W_{13}) = V_1 \cap (V_2 + \mathbb{F}_2 \cdot (v_1 + v_2)) \cap (V_3 + \mathbb{F}_2 \cdot (v_1 + v_3)) = V_1 \cap (V_2 + \mathbb{F}_2 \cdot v_1) \cap (V_3 + \mathbb{F}_2 \cdot v_1) = \mathbb{F}_2 v_1$, so that $D = \dim(H_1) = 1$. In both cases, $d = 3$, $d_{ij} = 1$, and $d_i = 0$, but the two cases have different values of d , namely $\check{d} = 3$ in the first case and $\check{d} = 2$ in the second. So, by Lemma 6, they have different values of D .