

# Diagnóstico de CSM en estegoanálisis

Daniel Lerch Hostalot  
David Megías Jiménez

XV Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2018)  
Granada, 3-5 octubre 2018



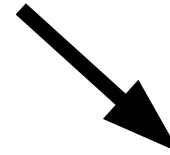
# Introducción

## ESTEGANOGRAFÍA



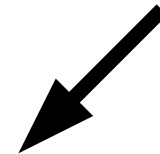
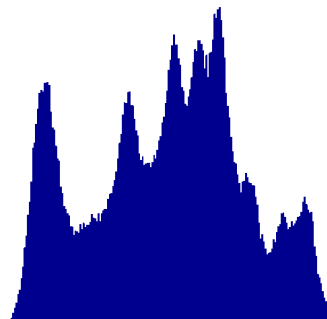
+

```
00101011110  
00111011110  
01101001110  
11100101110  
00100101111  
00100101000
```



## ESTEGOANÁLISIS

Información  
oculta?

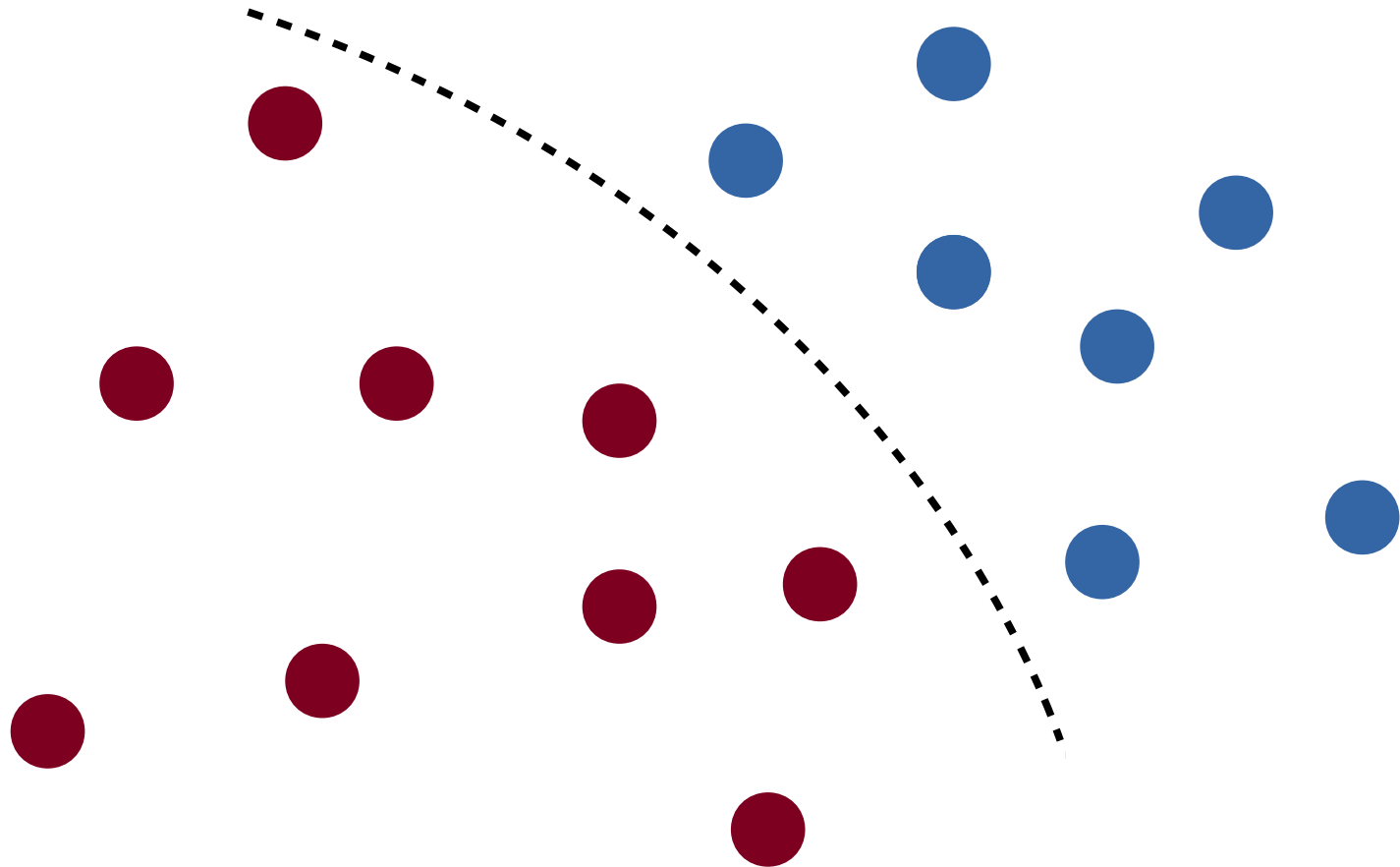


# ***Machine Learning*** **en estegoanálisis**

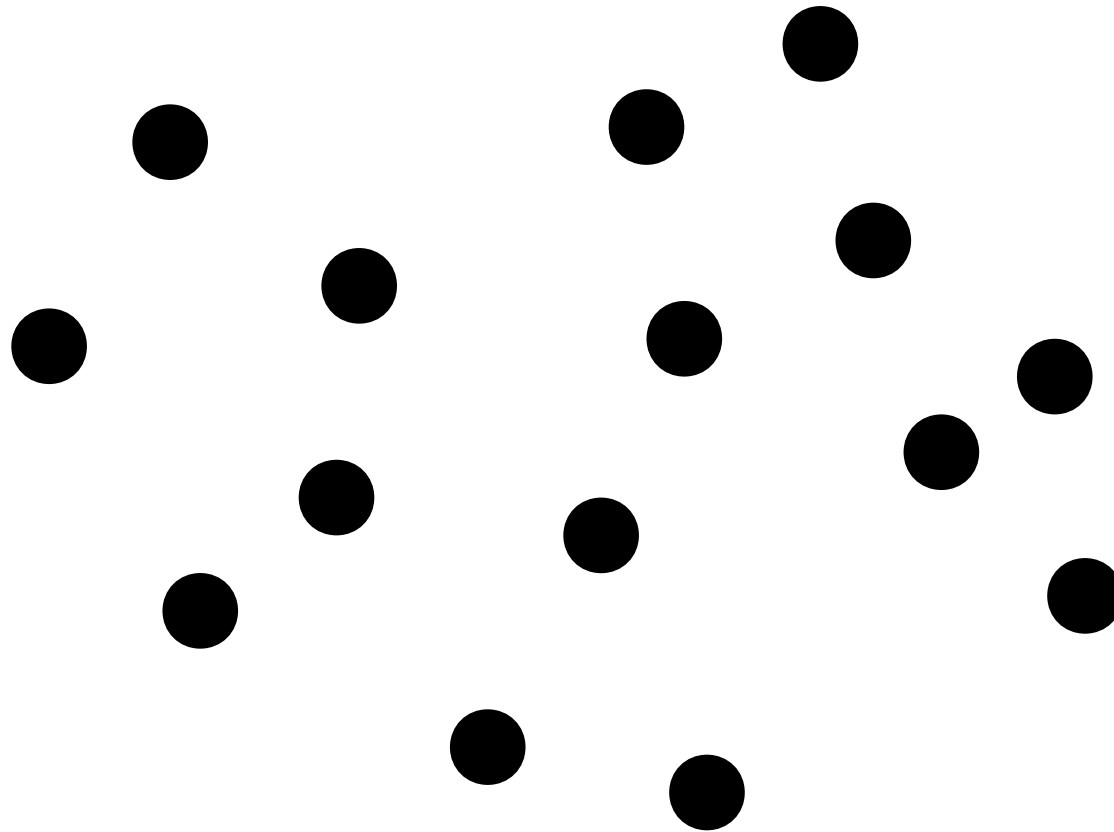
## CONJUNTO DE ENTRENAMIENTO

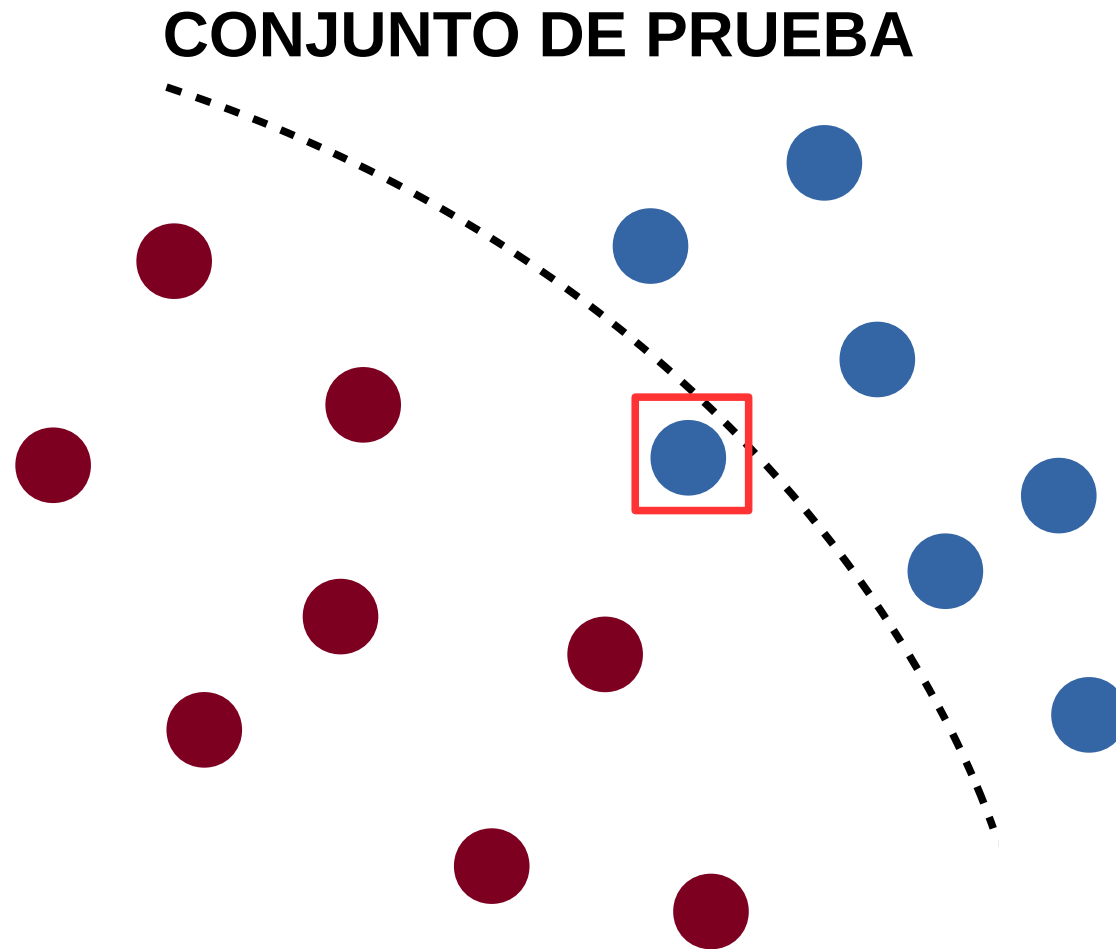


## CONJUNTO DE ENTRENAMIENTO



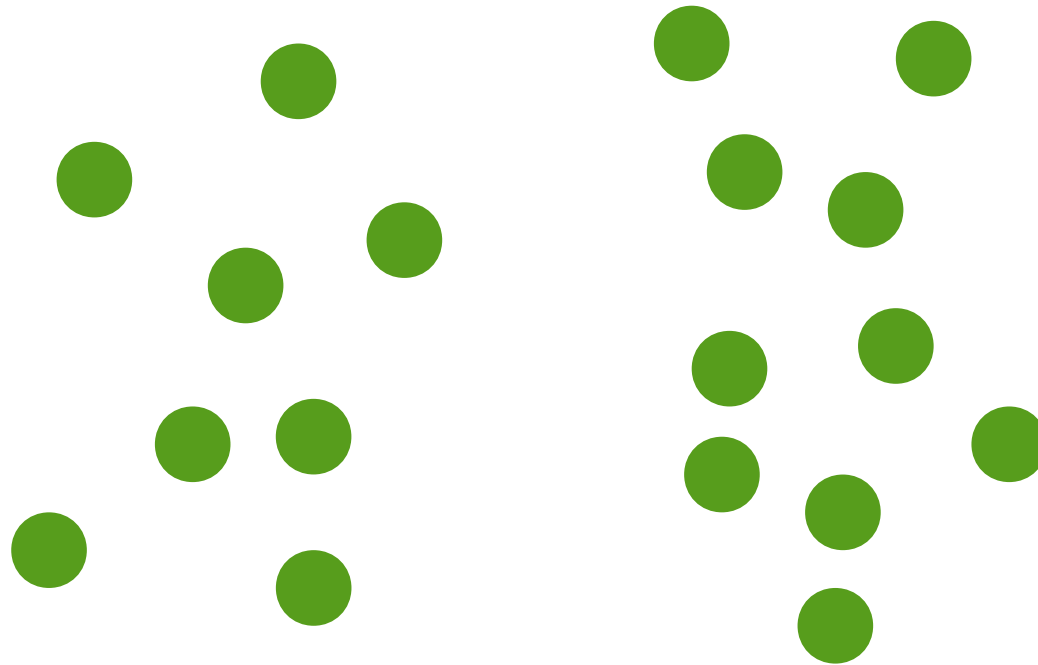
## CONJUNTO DE PRUEBA



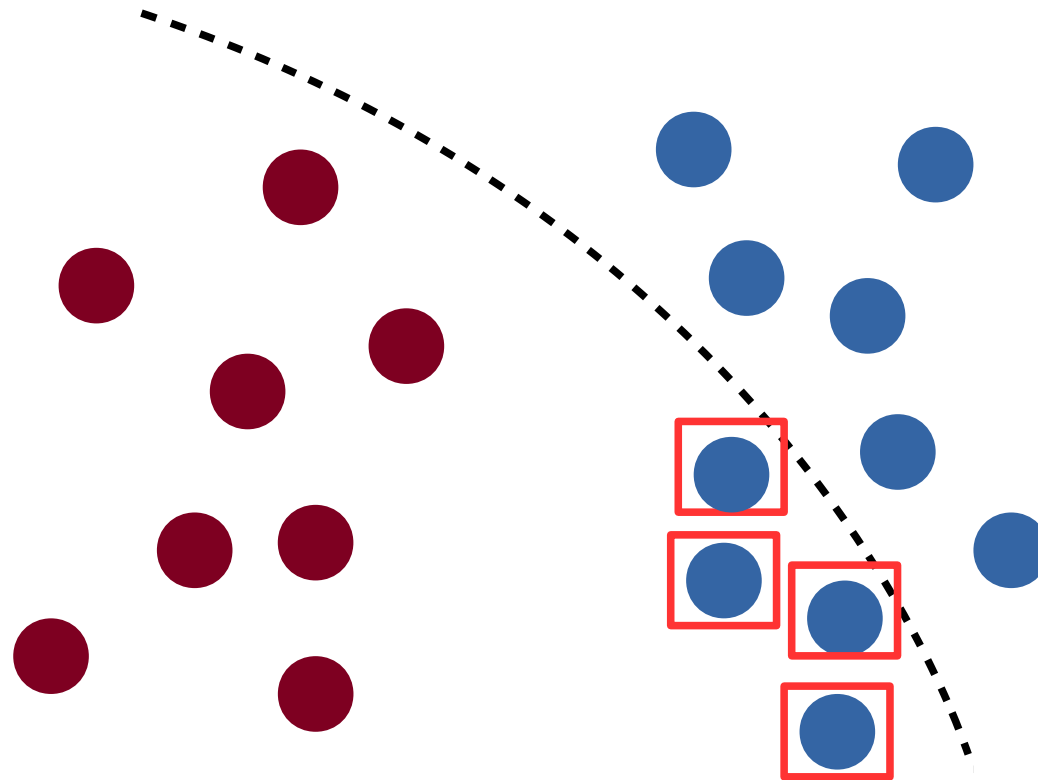




## CONJUNTO DE PRUEBA DE UN DOMINIO DIFERENTE



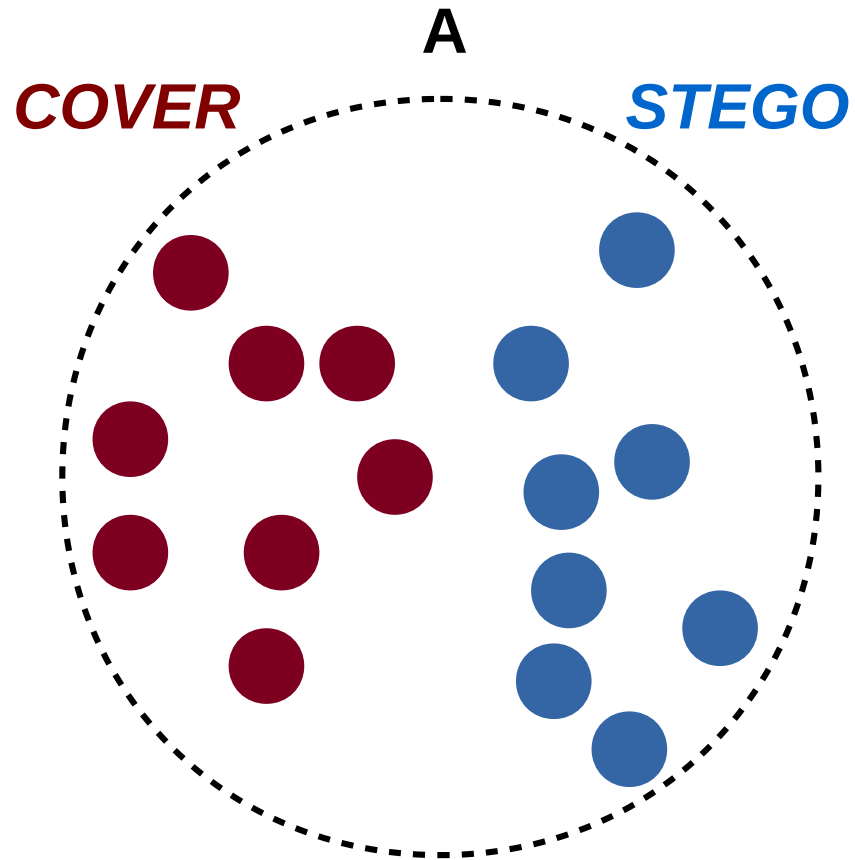
**CONJUNTO DE PRUEBA  
DE UN DOMINIO DIFERENTE**

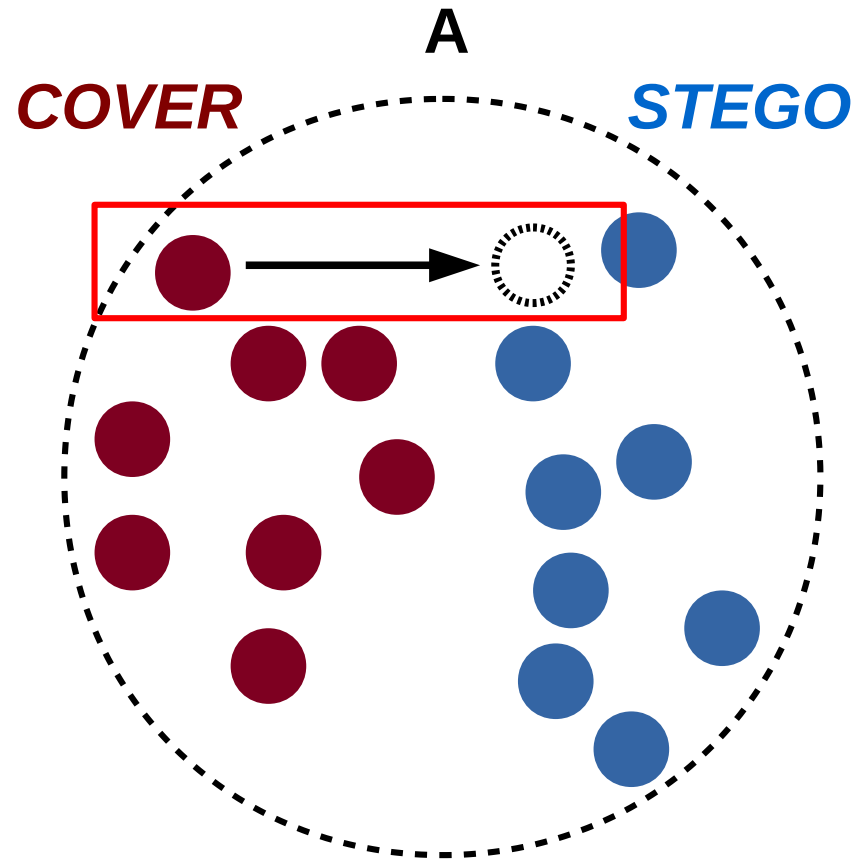


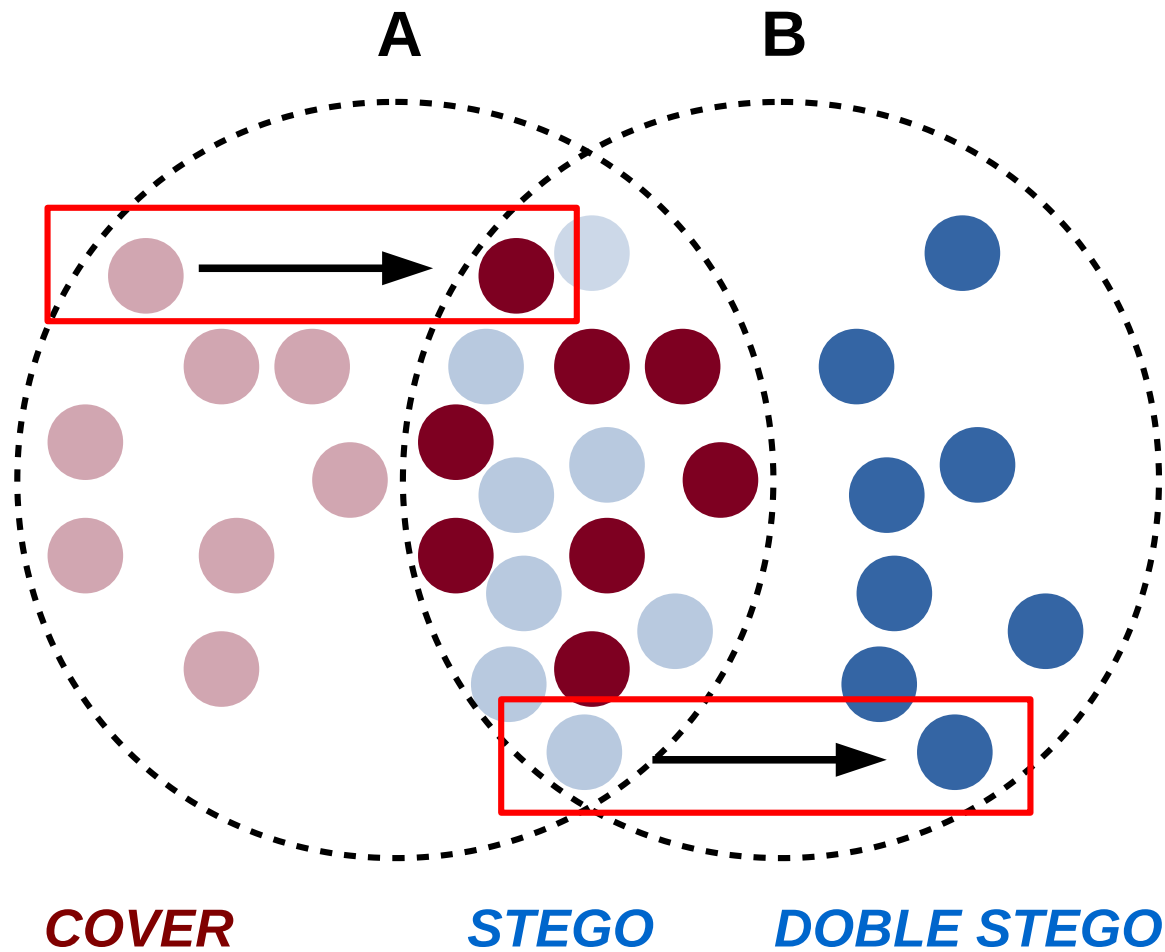
***COVER SOURCE MISMATCH (CSM)***

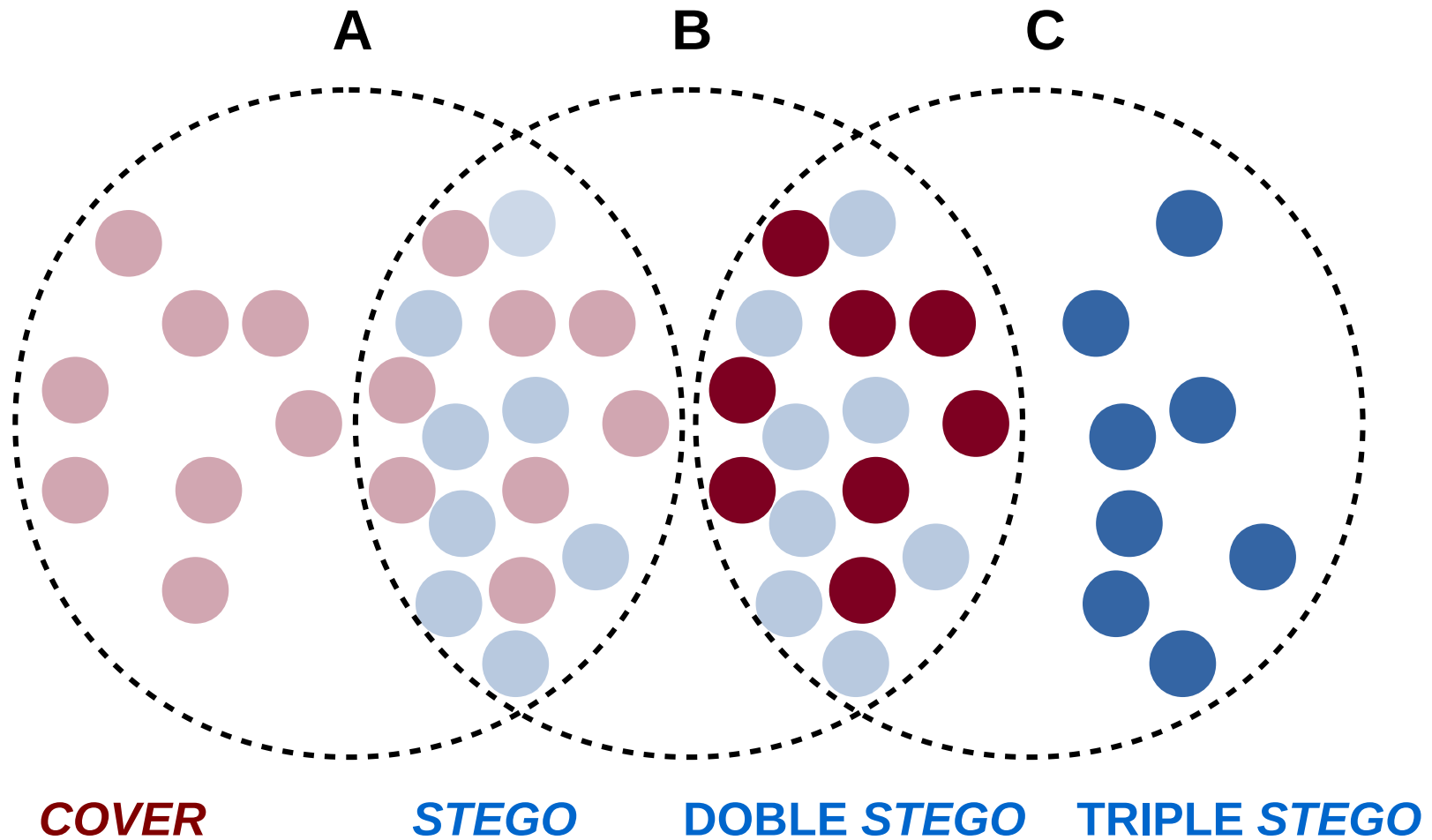
# NASD

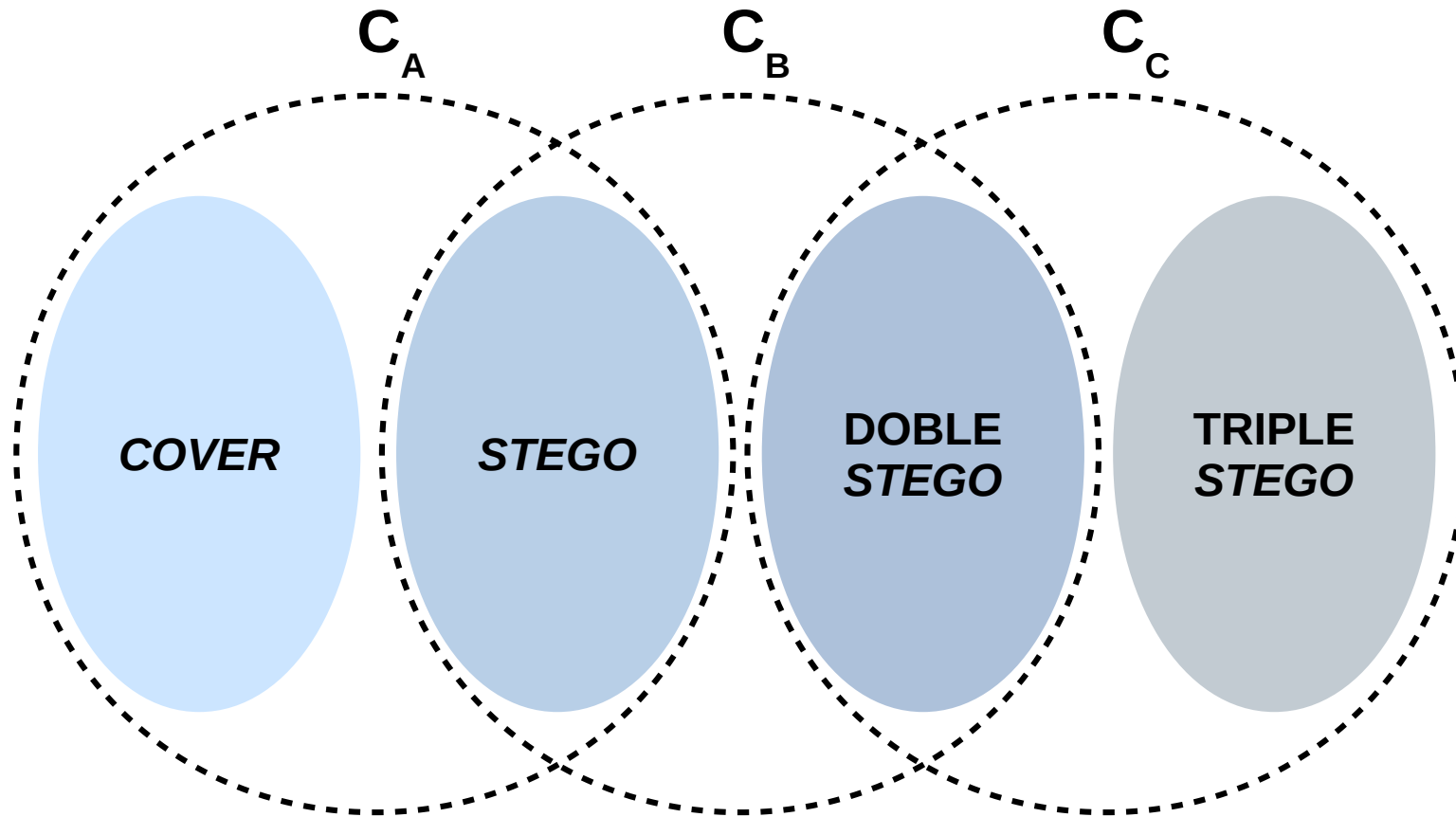
*Non-Aligned Sample Detection*





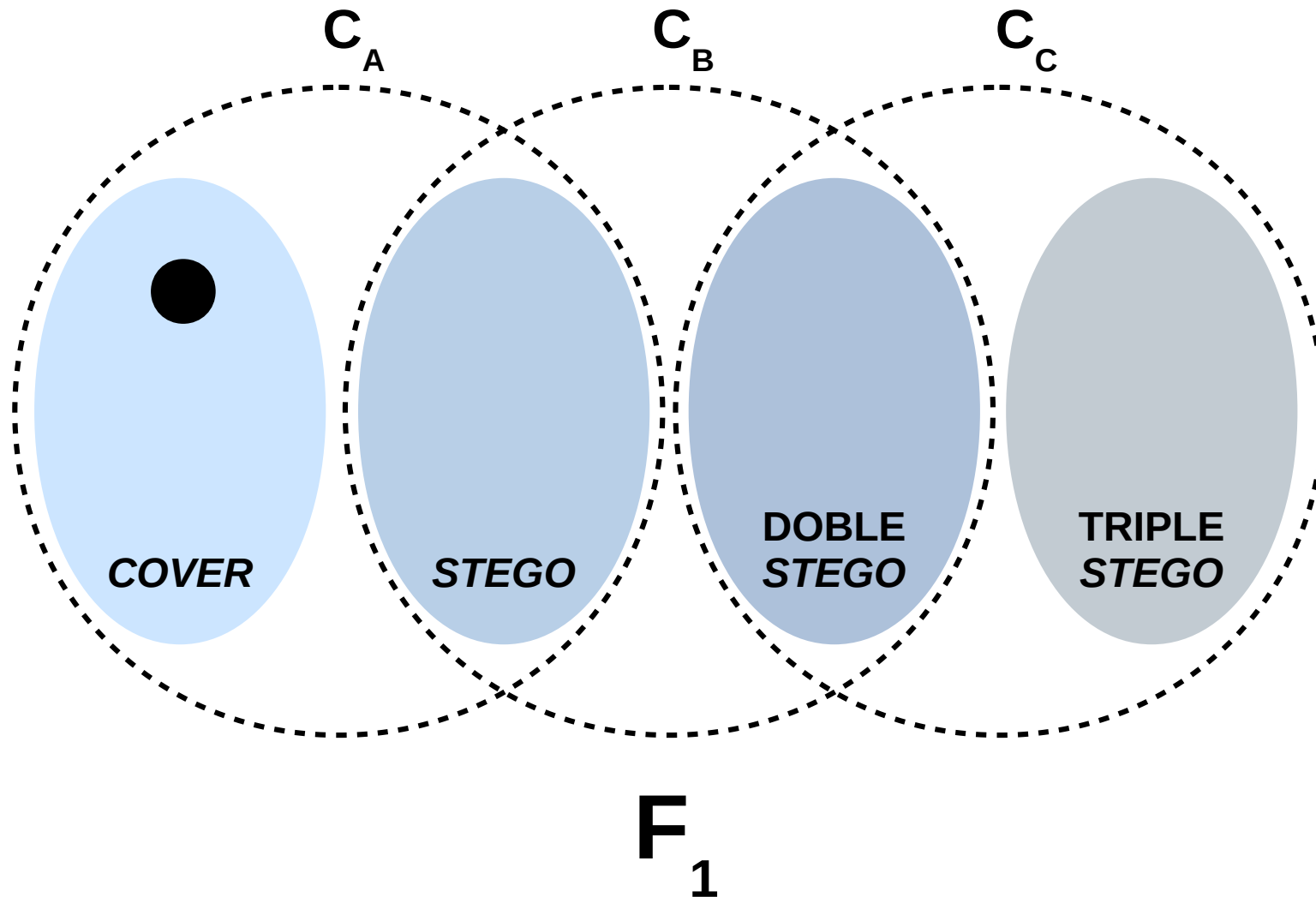


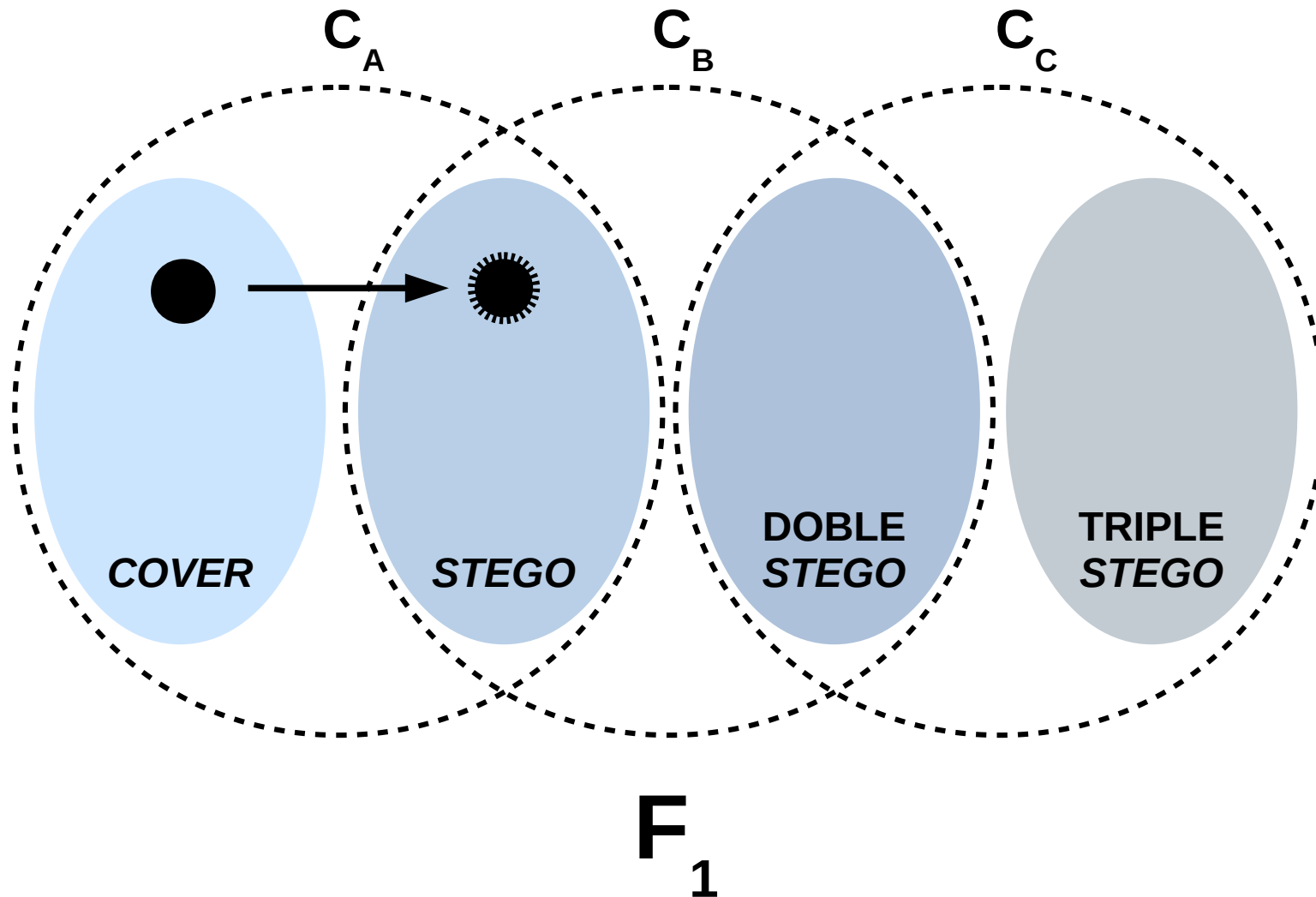


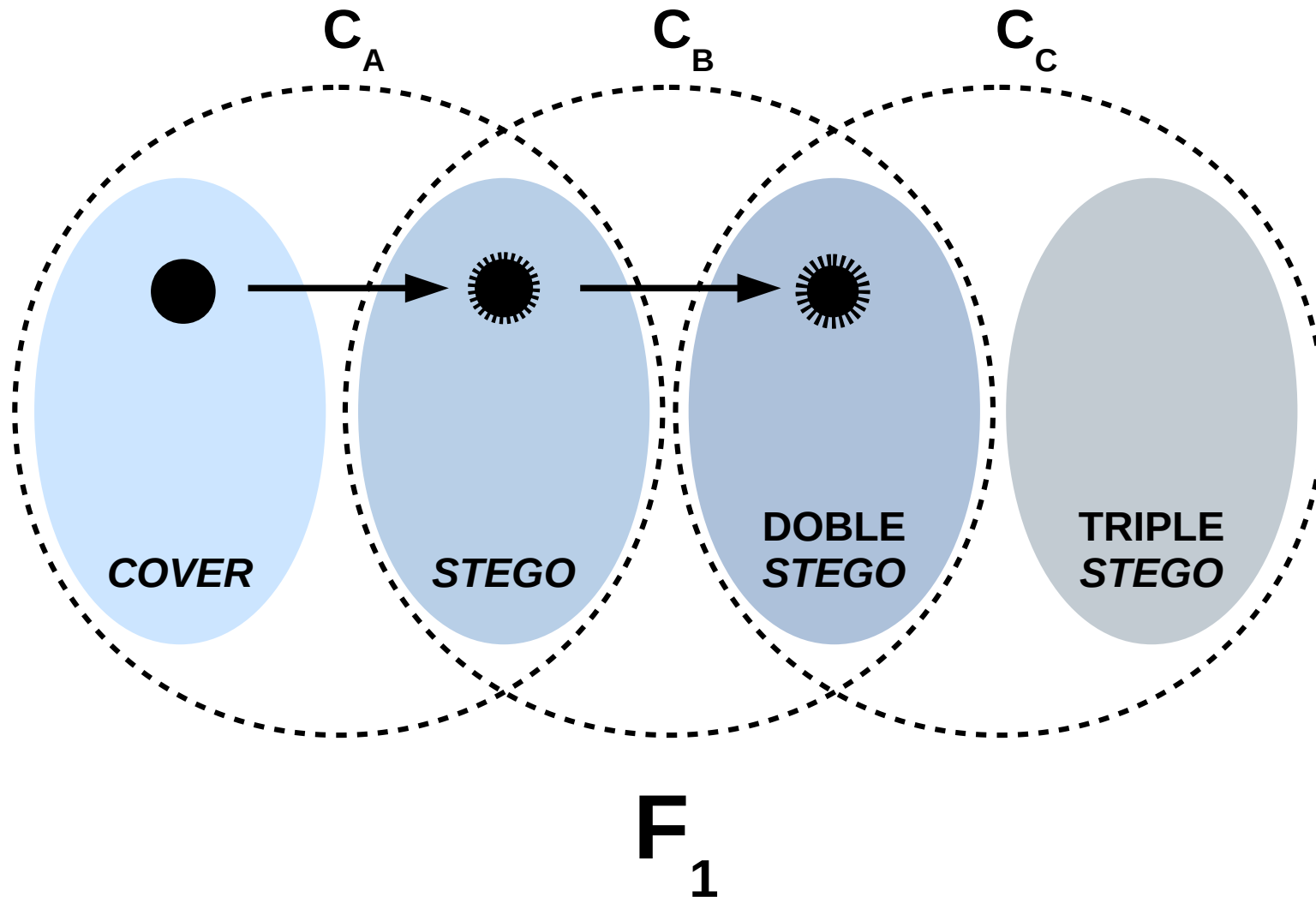


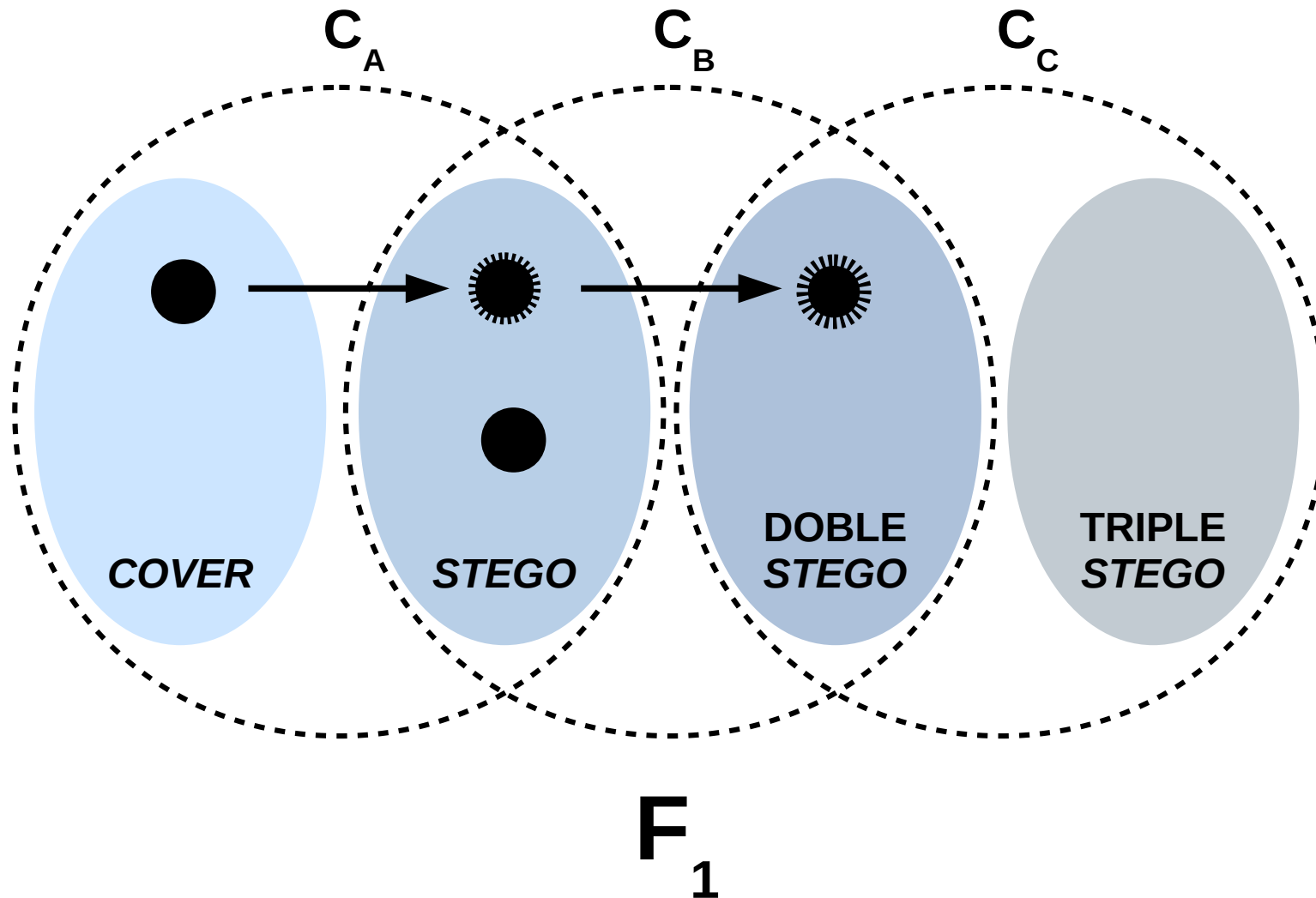
## CLASIFICADORES

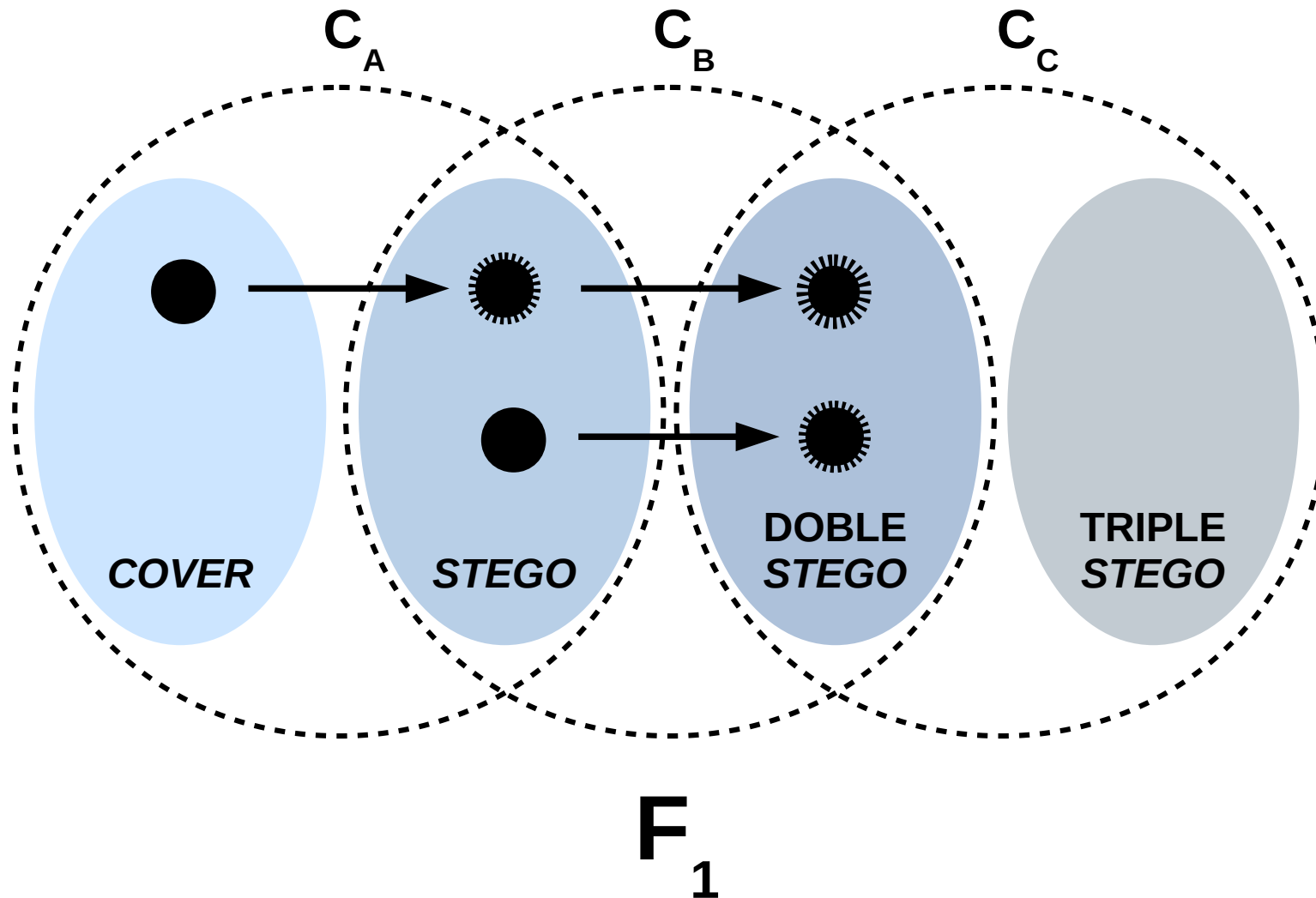


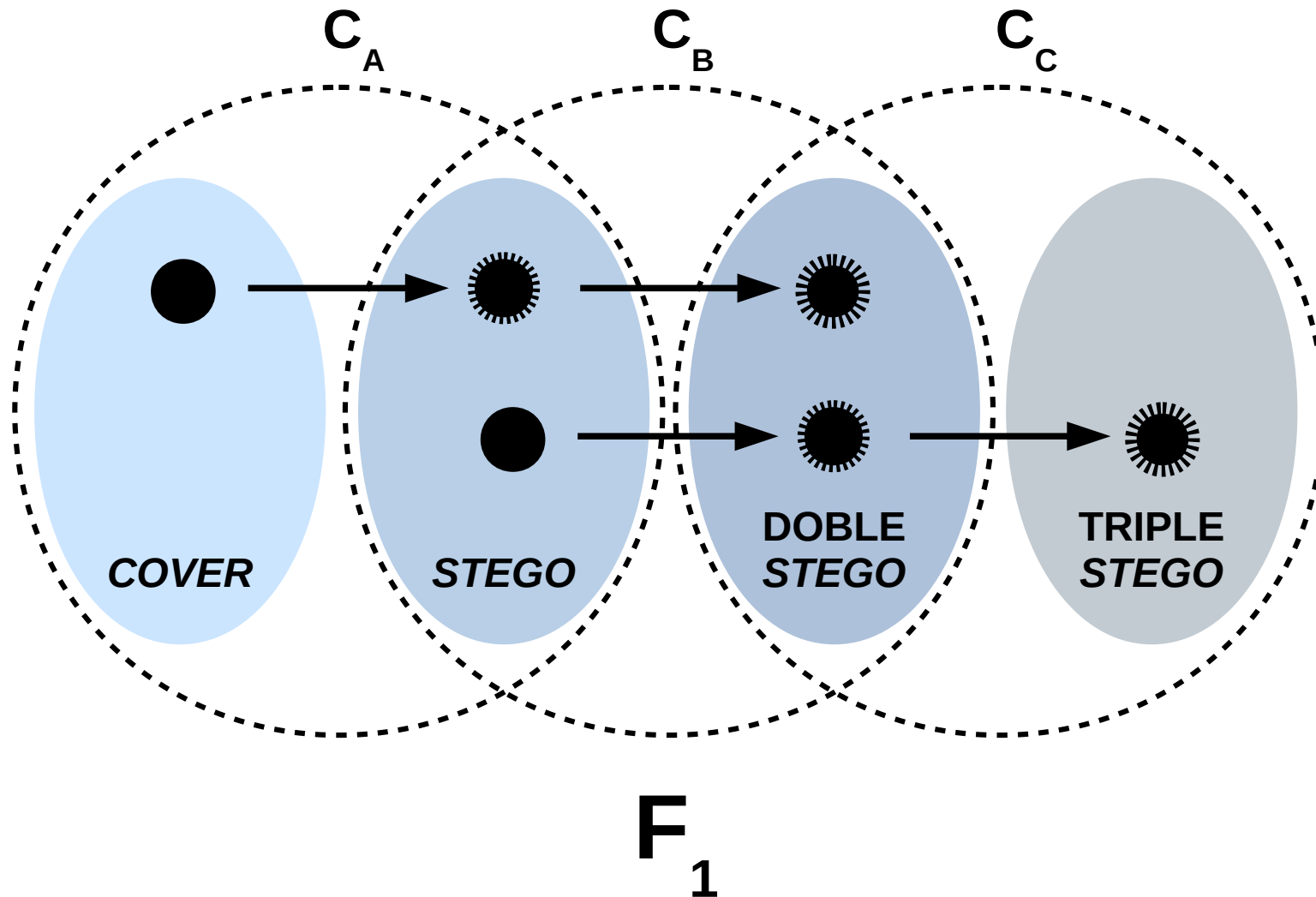


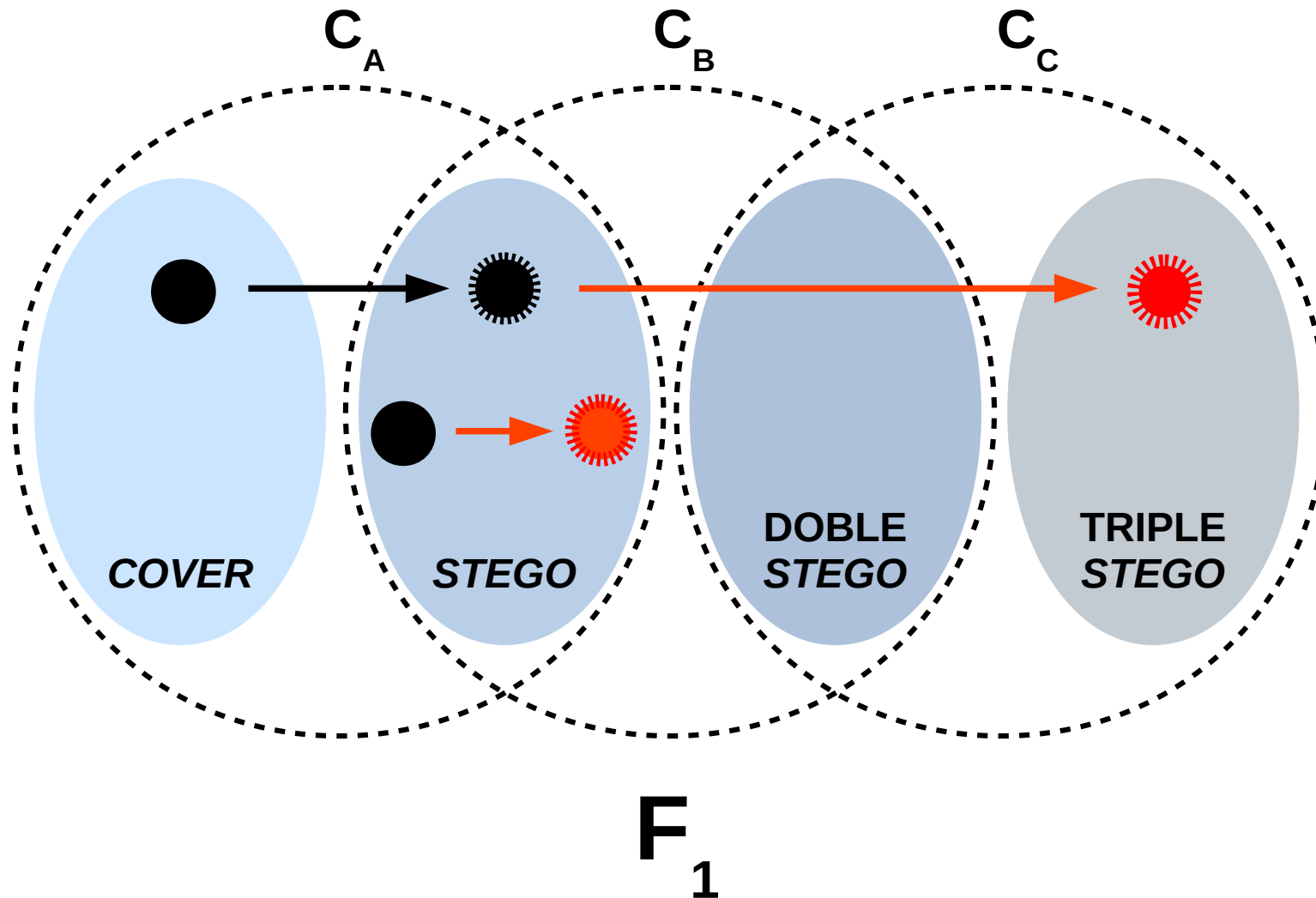


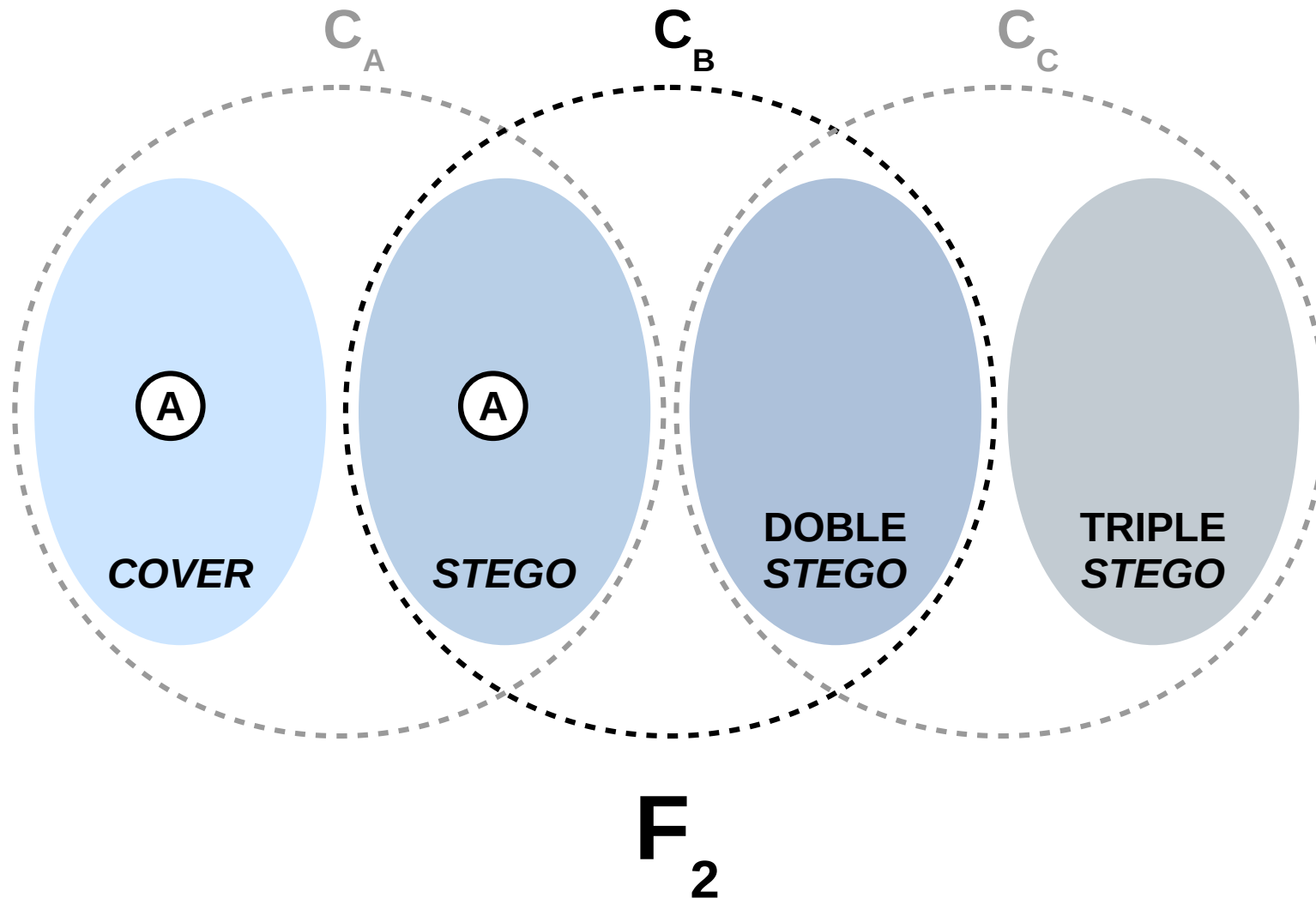




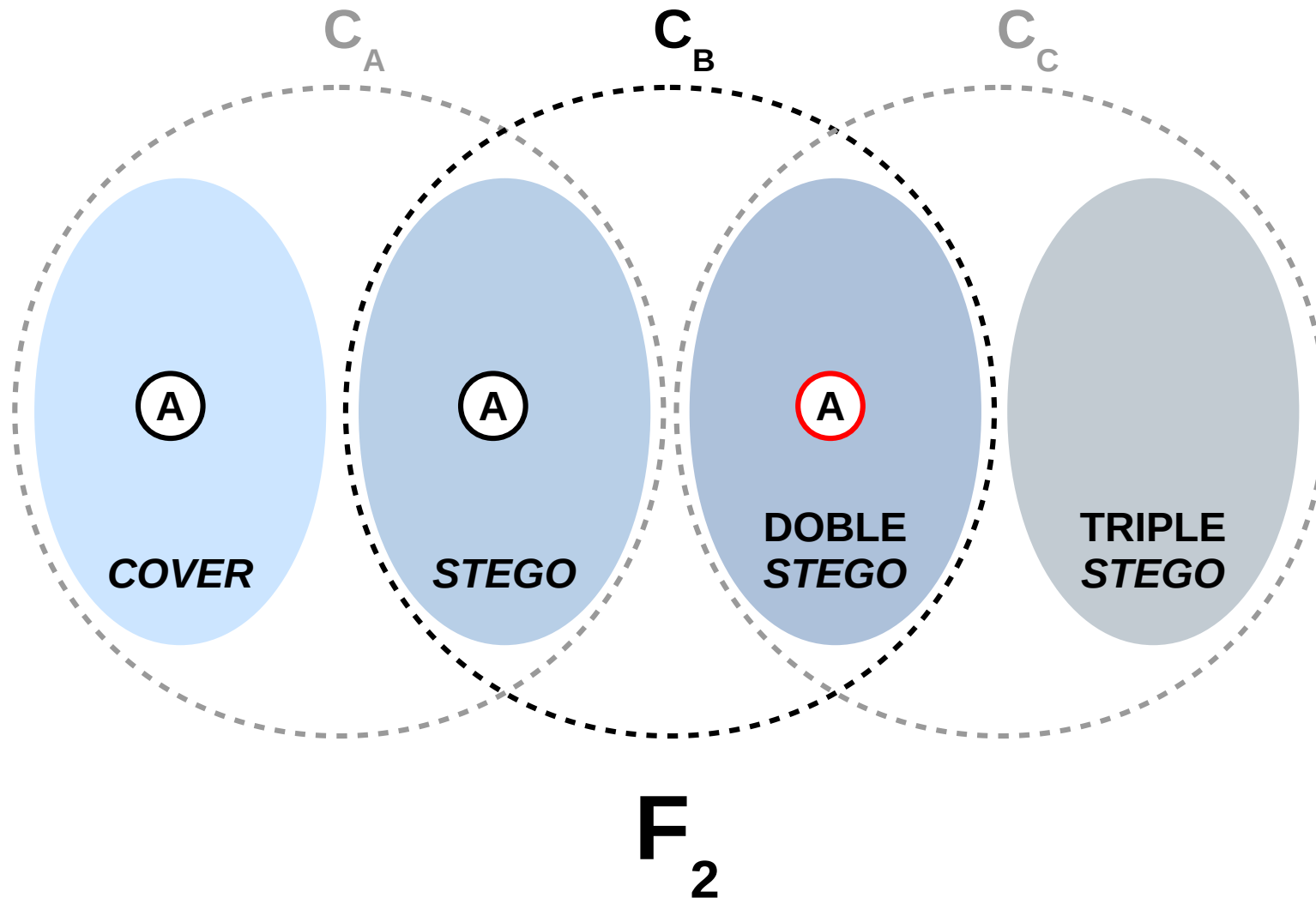


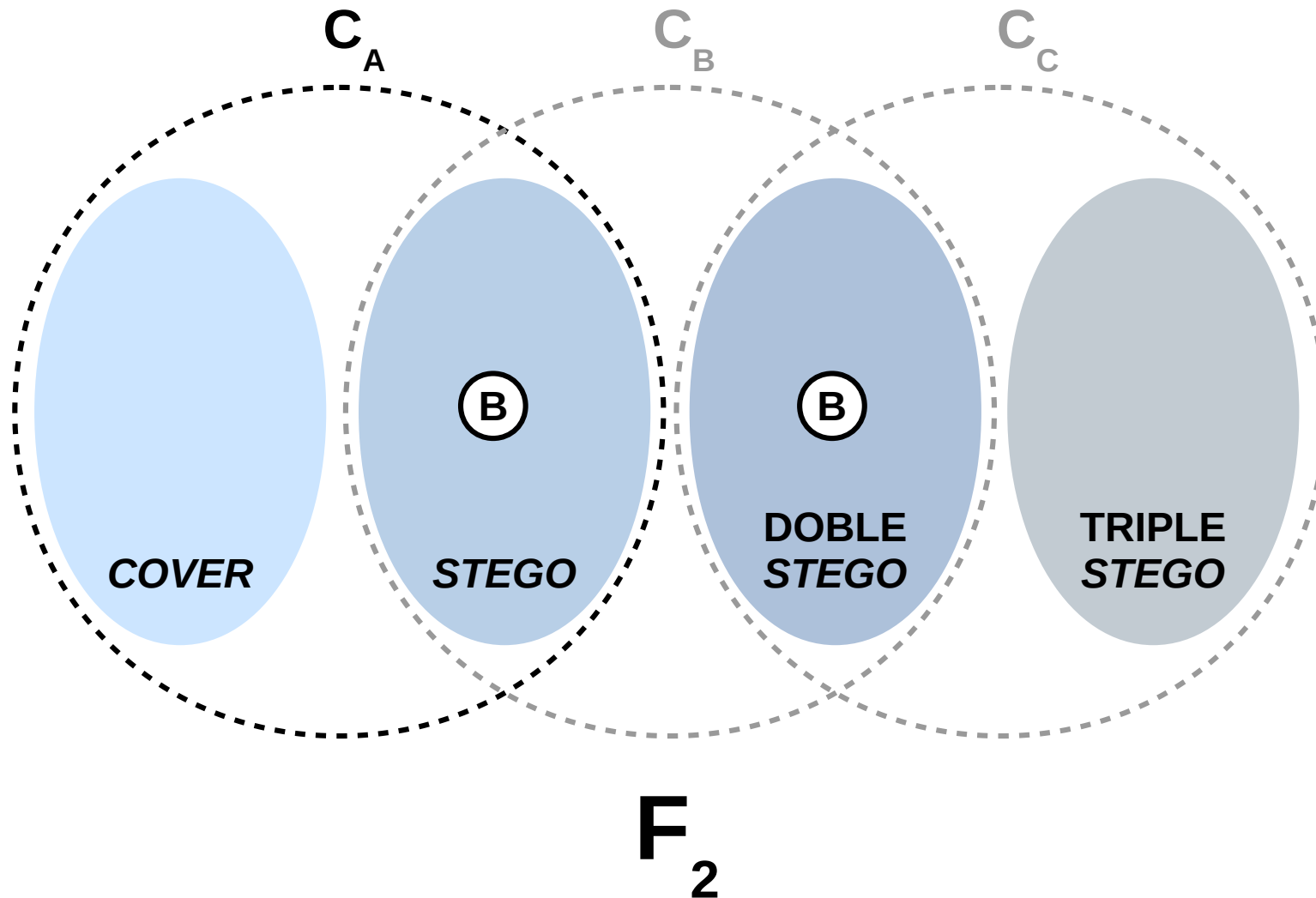


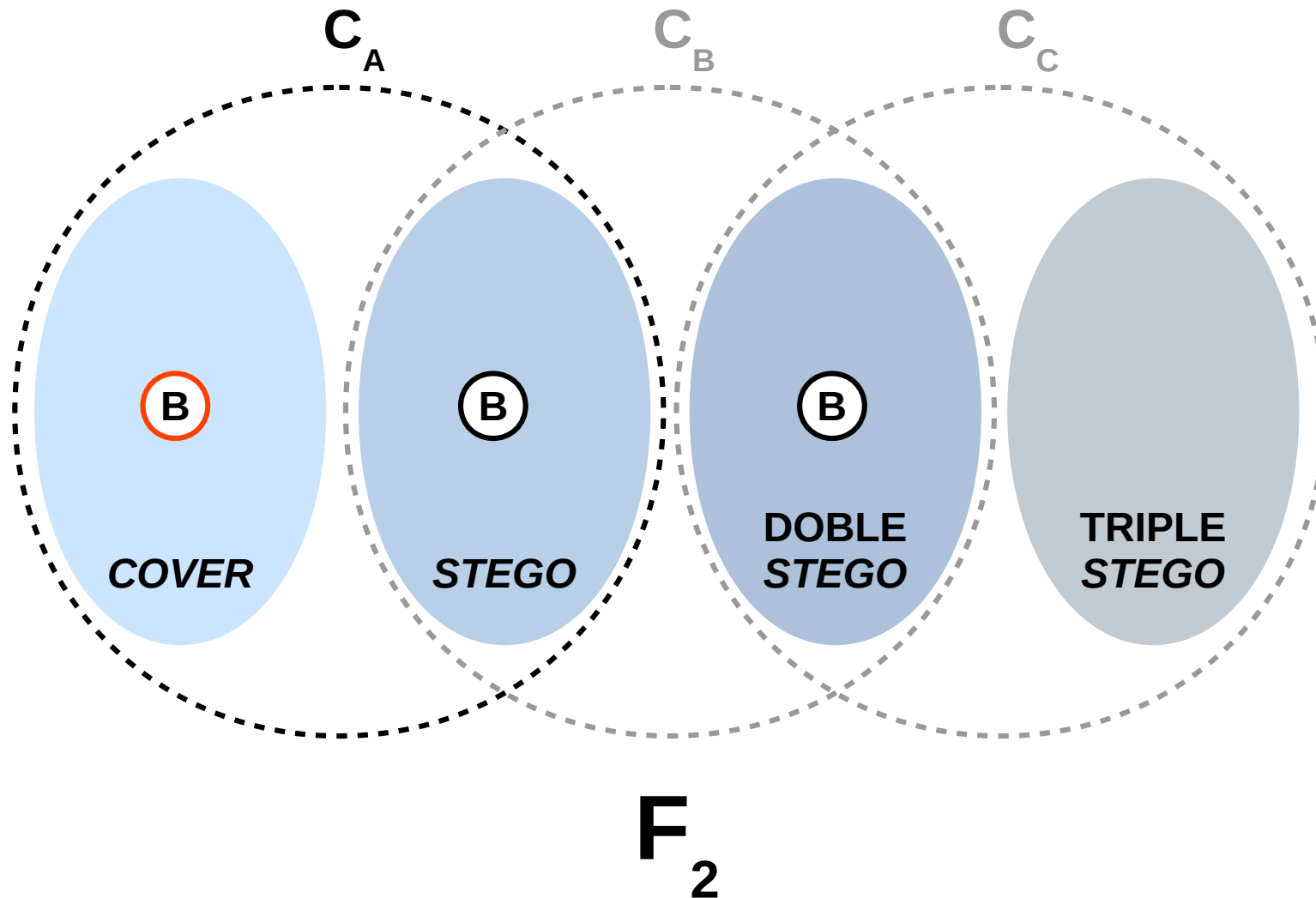


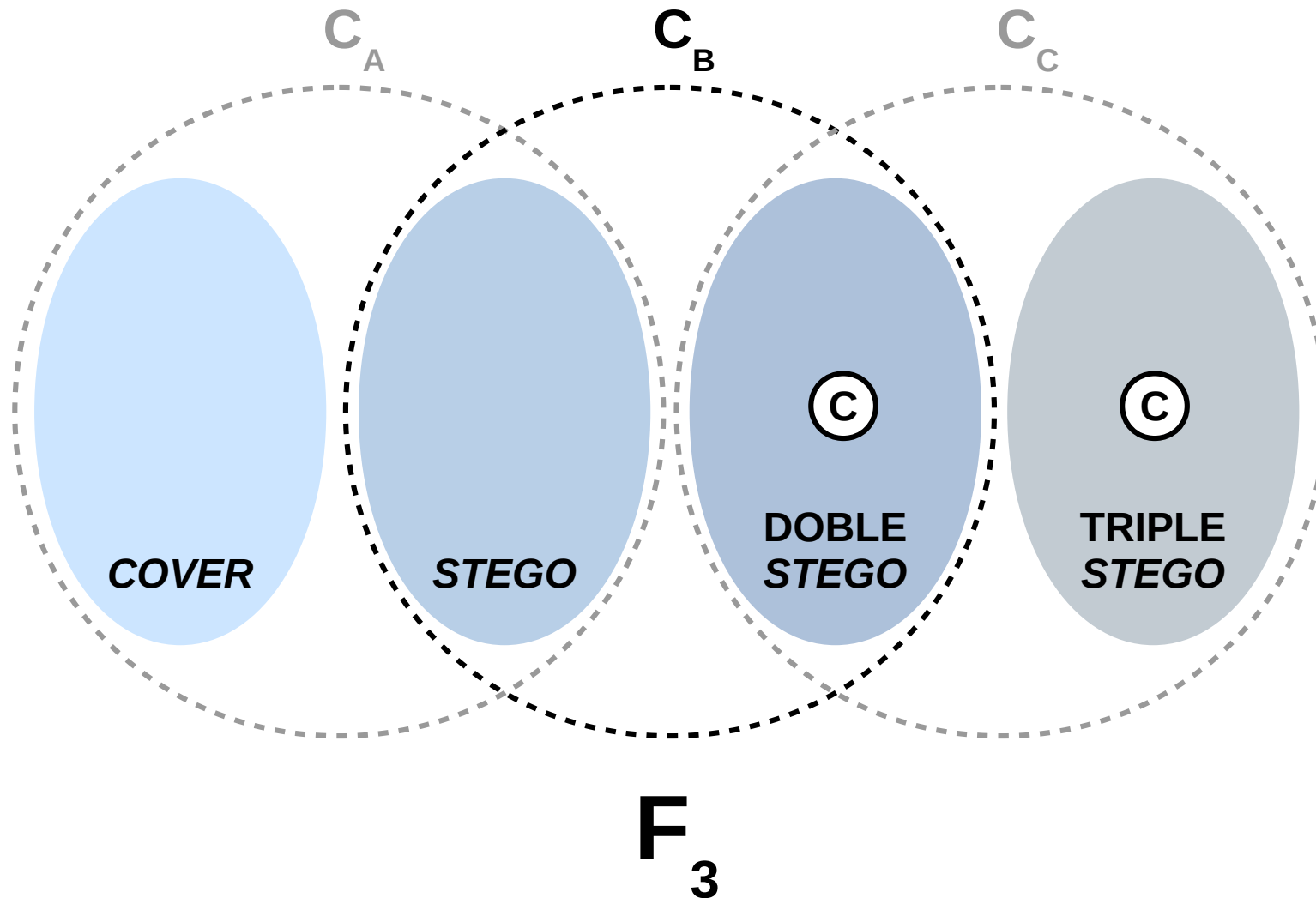


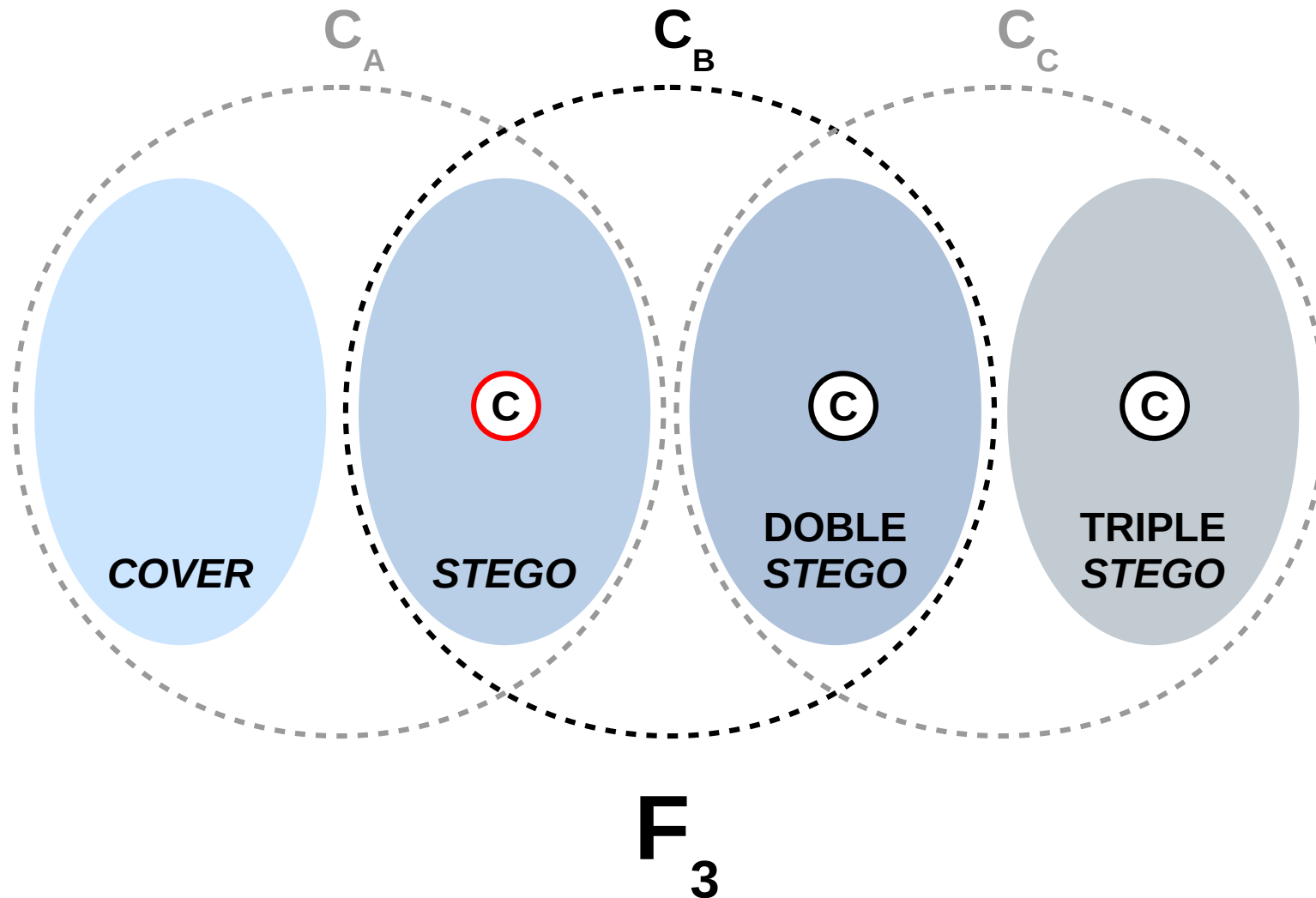


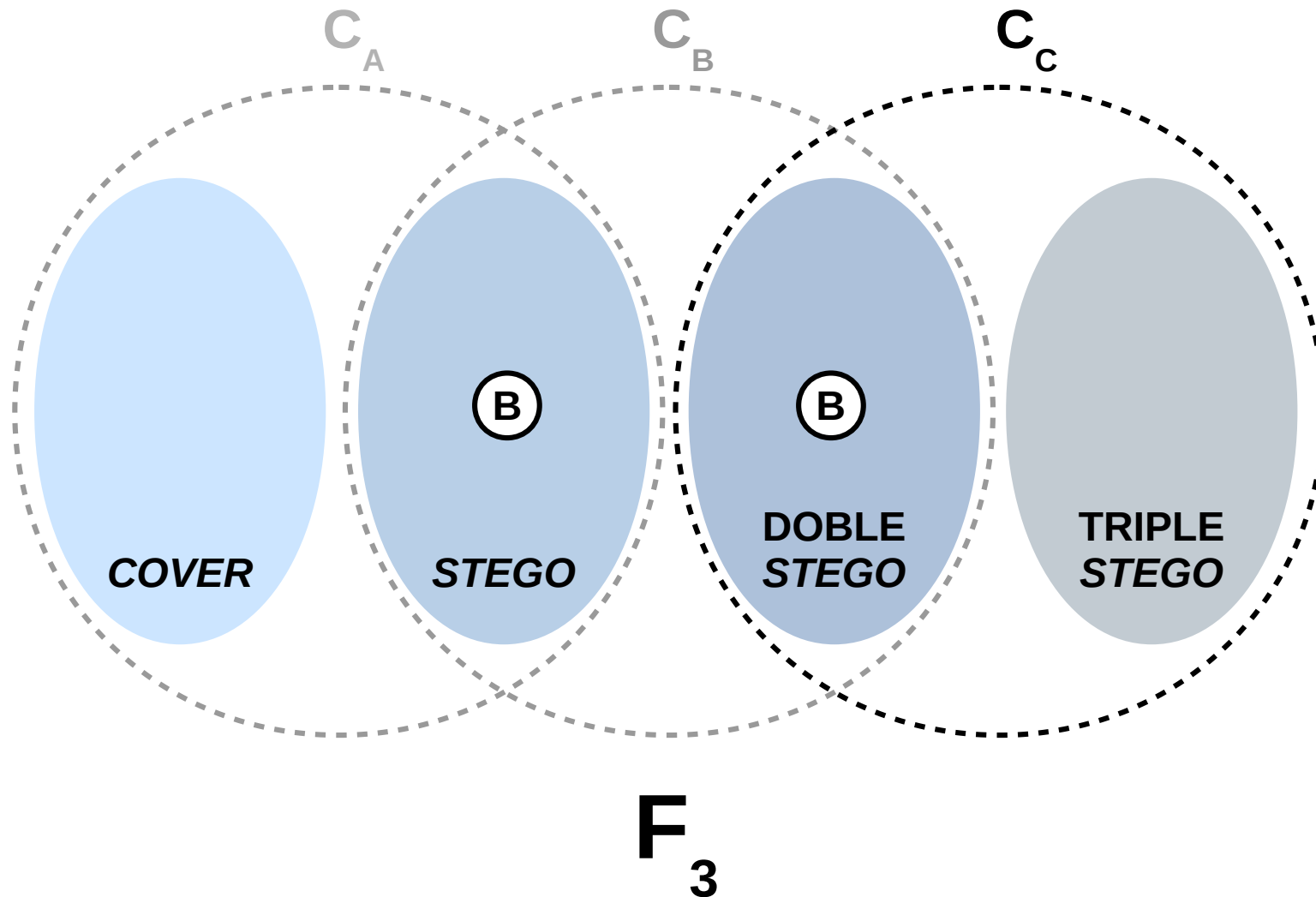


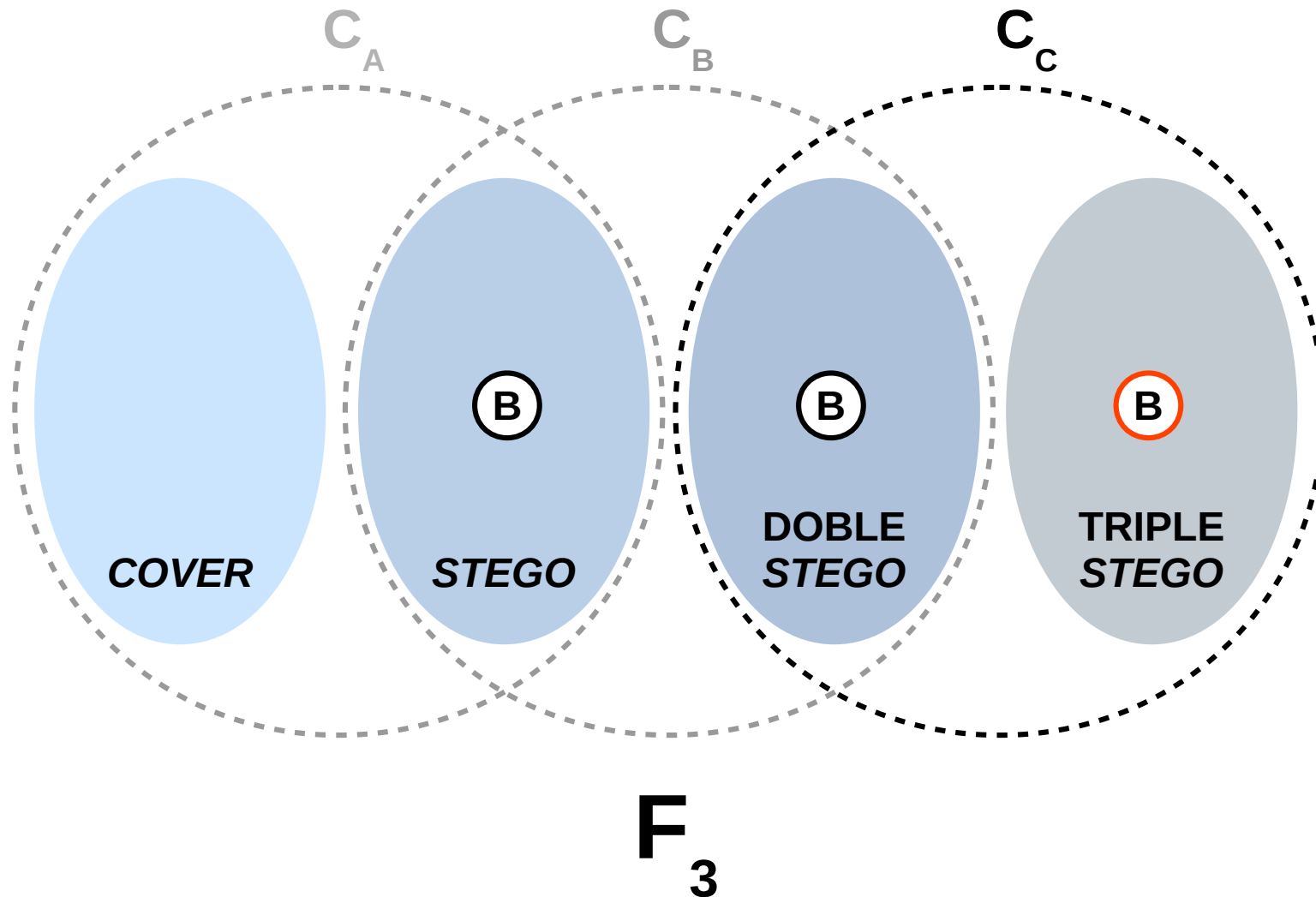












# FILTROS:

- Filtro *SOFT*:  $F_1$
- Filtro *MEDIUM*:  $F_1 + F_2$
- Filtro *HARD*:  $F_1 + F_2 + F_3$



# Resultados

Tabla I  
RESULTADOS DE CLASIFICACIÓN PARA NASD

ALGO	BR	Train DB	Test DB	RM+EC Err	H-NASD							M-NASD							S-NASD						
					Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC	Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC	Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC
HUGO	0.4	BOSS	BOSS	0.11	0.04	0.03	74	87	3	4	82	0.04	0.03	78	95	3	5	69	0.05	0.04	93	105	5	6	41
HUGO	0.4	BOSS	ALBI	0.07	0.05	0.02	41	43	4	0	162	0.04	0.02	57	45	4	0	144	0.06	0.04	57	110	5	5	73
HUGO	0.4	BOSS	CALP	0.25	0.16	0.02	14	12	4	1	219	0.17	0.03	26	13	7	1	203	0.16	0.06	32	55	14	2	147
HUGO	0.4	BOSS	ESO	0.50	0.00	0.00	2	1	0	0	247	0.00	0.00	2	1	0	0	247	0.40	0.02	2	4	0	4	240
HUGO	0.4	BOSS	INTE	0.50	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250
HUGO	0.4	BOSS	NOAA	0.50	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250
HUGO	0.2	BOSS	BOSS	0.22	0.10	0.03	37	38	2	6	167	0.00	0.06	43	54	3	13	137	0.13	0.09	60	84	6	16	84
HUGO	0.2	BOSS	ALBI	0.35	0.43	0.12	7	34	11	20	178	0.45	0.16	8	40	16	24	162	0.41	0.21	31	46	21	32	120
HUGO	0.2	BOSS	CALP	0.39	0.50	0.01	0	2	2	0	246	0.75	0.02	0	2	3	3	242	0.34	0.08	11	29	10	11	189
HUGO	0.2	BOSS	ESO	0.47	0.00	0.00	0	2	0	0	248	0.00	0.00	1	2	0	0	247	0.44	0.15	1	47	0	38	164
HUGO	0.2	BOSS	INTE	0.47	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.48	0.34	0	93	1	85	71
HUGO	0.2	BOSS	NOAA	0.49	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.49	0.30	0	77	0	75	98
WOW	0.4	BOSS	BOSS	0.16	0.05	0.02	55	65	2	4	124	0.07	0.04	62	75	2	8	103	0.10	0.08	77	98	7	13	55
WOW	0.4	BOSS	ALBI	0.50	0.40	0.01	3	0	2	0	245	0.76	0.05	4	0	13	0	233	0.72	0.05	4	1	13	0	232
WOW	0.4	BOSS	CALP	0.50	1.00	0.00	0	0	1	0	249	1.00	0.00	0	0	1	0	249	0.50	0.00	0	1	1	0	248
WOW	0.4	BOSS	ESO	0.43	0.00	0.00	0	1	0	0	249	0.00	0.00	0	1	0	0	249	0.46	0.21	0	62	0	52	136
WOW	0.4	BOSS	INTE	0.50	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.59	0.08	0	13	0	19	218
WOW	0.4	BOSS	NOAA	0.50	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.58	0.30	0	54	0	74	122
WOW	0.2	BOSS	BOSS	0.33	0.12	0.01	6	9	1	1	233	0.31	0.06	14	19	8	7	202	0.28	0.14	30	57	16	18	129
WOW	0.2	BOSS	ALBI	0.48	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.48	0.10	0	28	0	26	196
WOW	0.2	BOSS	CALP	0.51	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.50	0.02	2	4	1	5	238
WOW	0.2	BOSS	ESO	0.50	0.00	0.00	0	0	0	0	250	0.77	0.04	3	0	10	0	237	0.55	0.09	8	11	16	7	208
WOW	0.2	BOSS	INTE	0.50	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.63	0.04	5	1	7	3	234
WOW	0.2	BOSS	NOAA	0.48	0.00	0.00	0	0	0	0	250	0.68	0.06	7	0	15	0	228	0.54	0.22	36	12	41	15	146
UNIW	0.4	BOSS	BOSS	0.13	0.06	0.04	59	72	2	7	110	0.07	0.04	68	78	2	9	93	0.09	0.08	88	99	6	13	44
UNIW	0.4	BOSS	ALBI	0.28	0.42	0.04	7	8	7	4	224	0.63	0.11	8	8	23	4	207	0.36	0.16	8	63	23	17	139
UNIW	0.4	BOSS	CALP	0.46	0.56	0.02	3	1	4	1	241	0.61	0.09	10	4	21	1	214	0.54	0.12	16	9	28	1	196
UNIW	0.4	BOSS	ESO	0.44	0.50	0.00	0	1	1	0	248	0.67	0.02	0	2	4	0	244	0.48	0.12	1	32	4	27	186
UNIW	0.4	BOSS	INTE	0.47	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.62	0.10	0	15	0	24	211
UNIW	0.4	BOSS	NOAA	0.38	0.00	0.00	0	0	0	0	250	1.00	0.00	0	0	1	0	249	0.44	0.14	0	46	1	35	168
UNIW	0.2	BOSS	BOSS	0.24	0.12	0.03	21	29	1	6	193	0.15	0.05	33	37	2	10	168	0.13	0.07	54	71	3	15	107
UNIW	0.2	BOSS	ALBI	0.44	0.36	0.02	5	2	2	2	239	0.48	0.10	10	17	7	18	198	0.47	0.15	25	18	19	19	169
UNIW	0.2	BOSS	CALP	0.48	0.00	0.00	0	1	0	0	249	0.60	0.01	1	1	3	0	245	0.44	0.03	6	4	8	0	232
UNIW	0.2	BOSS	ESO	0.47	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.44	0.08	1	24	1	19	205
UNIW	0.2	BOSS	INTE	0.51	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.78	0.03	0	2	1	6	241
UNIW	0.2	BOSS	NOAA	0.51	0.00	0.00	0	0	0	0	250	0.00	0.00	0	0	0	0	250	0.49	0.08	0	21	0	20	209
TOTAL				0.40	0.12		334	408	49	56		0.21		435	494	148	103		0.32		648	1396	258	702	

Tabla I

# Diagnóstico de CSM en estegoanálisis

## Mejora del conjunto de entrenamiento

ALGO	BR	Train	Test	RM+EC	H-NASD						
		DB	DB	Err	Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC
HUGO	0.40	BOSS	CALP	0.25	0.16	0.02	14	12	4	1	219
HUGO	0.40	BOSS+ALBI	CALP	0.23	0.12	0.03	29	29	3	5	184
HUGO	0.40	BOSS+ESO	CALP	0.23	0.06	0.01	29	31	4	0	186
HUGO	0.40	BOSS+NOAA	CALP	0.34	0.66	0.06	5	3	16	0	226
HUGO	0.40	BOSS+INTE	CALP	0.25	0.36	0.03	8	6	7	1	228
HUGO	0.40	BOSS+ALBI+ESO	CALP	0.21	0.07	0.02	40	39	3	3	165
HUGO	0.40	BOSS+ALBI+ESO+NOAA	CALP	0.18	0.07	0.02	40	41	2	5	160
HUGO	0.40	BOSS+ALBI+ESO+NOAA+INTE	CALP	0.20	0.09	0.03	36	39	2	6	167

## Mejora del conjunto de entrenamiento

ALGO	BR	Train	Test	RM+EC	H-NASD						
		DB	DB	Err	Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC
HUGO	0.40	BOSS	CALP	0.25	0.16	0.02	14	12	4	1	219
HUGO	0.40	BOSS+ALBI	CALP	0.23	0.12	0.03	29	29	3	5	184
HUGO	0.40	BOSS+ESO	CALP	0.23	0.06	0.01	29	31	4	0	186
HUGO	0.40	BOSS+NOAA	CALP	0.34	0.66	0.06	5	3	16	0	226
HUGO	0.40	BOSS+INTE	CALP	0.25	0.36	0.03	8	6	7	1	228
HUGO	0.40	BOSS+ALBI+ESO	CALP	0.21	0.07	0.02	40	39	3	3	165
HUGO	0.40	BOSS+ALBI+ESO+NOAA	CALP	0.18	0.07	0.02	40	41	2	5	160
HUGO	0.40	BOSS+ALBI+ESO+NOAA+INTE	CALP	0.20	0.09	0.03	36	39	2	6	167

## Mejora del conjunto de entrenamiento

ALGO	BR	Train	Test	RM+EC	H-NASD						
		DB	DB	Err	Err <sub>C</sub>	Err <sub>T</sub>	TP	TN	FP	FN	NC
HUGO	0.40	BOSS	CALP	0.25	0.16	0.02	14	12	4	1	219
HUGO	0.40	BOSS+ALBI	CALP	0.23	0.12	0.03	29	29	3	5	184
HUGO	0.40	BOSS+ESO	CALP	0.23	0.06	0.01	29	31	4	0	186
HUGO	0.40	BOSS+NOAA	CALP	0.34	0.66	0.06	5	3	16	0	226
HUGO	0.40	BOSS+INTE	CALP	0.25	0.36	0.03	8	6	7	1	228
HUGO	0.40	BOSS+ALBI+ESO	CALP	0.21	0.07	0.02	40	39	3	3	165
HUGO	0.40	BOSS+ALBI+ESO+NOAA	CALP	0.18	0.07	0.02	40	41	2	5	160
HUGO	0.40	BOSS+ALBI+ESO+NOAA+INTE	CALP	0.20	0.09	0.03	36	39	2	6	167

# Conclusiones y trabajo futuro

## Conclusiones:

- Método para diagnosticar CSM.
- Metodología para mejorar el conjunto de entrenamiento.
- Verificado con 5 bases datos y con diferentes algoritmos y *bitrates*.

## Trabajo futuro:

- Analizar si otras condiciones (como el uso de un algoritmo o bitrate incorrecto) producen muestras no alineadas.



# Diagnóstico de CSM en estegoanálisis

## Gracias por su atención

